AOA Tenant Screening

Comprehensive • Low Cost • 24/7 Instant Access

How it Works

Three-Step Accreditation Process:

STEP 1: SUBMIT ONLINE FORM

Complete this form as an individual owner or as a business entity. Make sure that the information you provide in this form is accurate and is consistent with your membership information.

STEP 2: VERIFY YOUR IDENTITY WITHIN SECONDS

Only AOA offers this express service for members interested in TransUnion Credit Reports. Further details are listed on the following page.

-OR- For Experian, upload, email, fax, or mail the required documents. Further details are listed on the following page.

STEP 3: PASS OFFICE SITE INSPECTION

To receive full credit reports, TransUnion requires just a one-time on-site visit for offices located at residential or commercial locations.

Experian requires an annual on-site inspection for residential locations and just a one-time site inspection for commercial locations. Go to **https://bit.ly/aoa-site-inspection** to order your site inspection today.

No site inspection needed for Experian ABC Grade Reports!

Landlord accreditation required for access to full credit reports.

The landlord accreditation process gives you access to instant full credit reports. This verification process is REQUIRED by TransUnion, and Experian, in accordance with the Fair Credit Reporting Act; it is required by law to ensure the safety of consumer credit information. If you need a screening report sooner, you can utilize AOA's ABC Grade Report.

Get Started Today!

Scan me

http://bit.ly/aoacrsa

For more information, please call **(800) 363-5296** or email **aoa.crsa@aoausa.com**.

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

PLEASE SELECT THE SERVICE(S) OF YOUR CHOICE

☐ JUST EVICTION AND/OR CRIMINAL REPORTS

No other steps required!

Just complete this form for access to AOA'S Double Whammy Eviction Reports and 3-in-1 Criminal Reports.

☐ NO SITE INSPECTION ABC GRADE REPORT

Follow Experian requirements with **no site inspection needed!**

This report summarizes the full credit report data into a grade-based credit rating. Upon request, you can even set the criteria yourself.

☐ TRANSUNION FULL CREDIT REPORT

Login to your AOA membership account, and press the "Verify ID" button on the main navigation bar to verify your identity with TransUnion. This technology will auto-fill your AOA Membership Account information into the verification form. A voice or text code will be sent to the phone number on file.

A **one-time** on-site visit is required to gain access to full credit reports for users that are operating as an individual owner or as a business entity. The fee for the site inspection is $64.

If you are operating under a business entity, please also submit ONE of the following: Business license, LLC documents, proof of fictitious name filing, OR a Federal Tax ID, letter the IRS sent when they assigned the Tax ID number showing your name and affiliation. Real estate firms must also include a broker's license.

If you have been in business less than a year, please also submit a utility bill for your physical address (where office/files are located).

Not Computer Savvy?

If you'd rather do physical paperwork, then you do not need to complete the online Verify ID but instead submit:

1) Copy of your driver's license.
2) Either a voided check, bank statement, or bank deposit slip
3) A phone bill.

All documents can be securely uploaded within your membership portal. You will find the "Upload documents" button on the main navigation bar. You can also email files to aoa.crsa@aoausa.com, fax them to 818-936-6703, or mail them to our office.

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

EXPERIAN FULL CREDIT REPORT

Complete the verification process as a Individual Owner or Business Entity by submitting:

1) Copy of your driver's license.
2) Either a voided check, bank statement, or bank deposit slip
3) A phone bill
4) If you are an individual owner or LLC, please also submit proof of ownership for each of your rental properties, such as property insurance or property tax bill per property.
5) One completed and signed rental application or lease agreement for each rental property (No more than three required in total for individual owners. Business entities require a total of three.)
6) If you are operating under a business entity, please also submit ONE of the following: business license, LLC documents, proof of fictitious name filing OR a Federal Tax ID letter the IRS sent when they assigned the Tax ID number, showing your name and affiliation. Real estate firms must also include a broker's license.

***Property Management Companies** submit a sample property management contract, active business license and are not required to provide proof of ownership for rental properties.

If you are operating from a **residential** location, a one-time on-site visit is required **annually**. If you are operating from a **commercial location**, a **one-time**, on-site visit is required. The inspection fee is $64.

All documents can be securely uploaded within your membership portal. You will find the "Upload documents" button on the main navigation bar. You can also email files to aoa.crsa@aoausa.com, fax them to 818-936-6703, or mail them into our office.

*** All Information must show a matching name, address, and phone number to the information provided on the agreement.**

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

COMPLETE END USER APPLICATION

RENTAL BUSINESS ENTITY OR INDIVIDUAL INFORMATION

Specify Type of Ownership: ☐ Individual Owner ☐ LLC ☐ Management Company ☐ Rental Corporation ☐ Real Estate Broker / Firm

Company/Individual Name: _____

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

Location where rental applications are stored: (no P.O. box numbers, please)

Physical Street Address : _____

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

Is this a residential address? ☐ Yes ☐ No

Previous Address: _____

City: _____ State: _____ ZIP: _____

Social Security Number: _____ Tax ID Number: _____

Tel: _____ Fax: _____ Email Address: _____

Have you been providing rental housing for more than one year? ☐ Yes ☐ No

Number of rental properties you own/manage: ☐ 1-4 ☐ 5-10 ☐ 11-25 ☐ over 25

Anticipated monthly credit reports: ☐ 0-5 ☐ 6-10 ☐ 11-24 ☐ over 24

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

Website Address: _____

PRINCIPAL OF THE COMPANY OR INDIVIDUAL OWNER

Principal name: _____ Title or Position: _____

Current Residential Street Address: _____

City: _____ State: _____ ZIP: _____

PERMISSIBLE PURPOSE/APPROPRIATE USE

Please indicate the specific purpose for which credit information will be used. This section **MUST** be completed.

☐ Tenant Screening ☐ Employment (TransUnion Only)

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 of 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 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

CREDIT REPORT SERVICE AGREEMENT & FCRA REQUIREMENTS

THIS AGREEMENT is between Apartment Owners Association of California, Inc. ("AOA") and _____ ("Client").
This Agreement is entered into on _____, 20____.

1. Services to be Provided by AOA_

A. Upon request and relying upon Client's representations that it has a legitimate purpose for information, AOA will provide background checks, verifications and other consumer reports to the Client when available. AOA will only furnish a report for a permissible purpose under the Fair Credit Reporting Act, 15 U.S.C. §1681 et seq. ("FCRA") and no other purpose.
B. Periodically and upon request, AOA will provide to Client copies of certifications, consumer consents, notices and summary of rights under the FCRA as well as other forms, which AOA finds helpful in meeting its obligations under the FCRA and other applicable laws. Client acknowledges receipt of the Consumer Financial Protection Bureau Notice of Consumer's Rights and Notice to Users.

2. Representations of Client when ordering reports

A. Client represents that it is an existing business with the legitimate need for verification and reports offered by AOA. The nature of Client's business is: _____.
Client specifically represents that reports will only be obtained for its own one time use and it is the end user of the reports. It will not further distribute, sell, give or trade such information with any third party. Notwithstanding the above, Client may share a report, except credit, for joint use as described in Section 2B below. Client will request and use reports for the following permissible purposes listed below.
B. Client may share reports with another entity for joint use. The FCRA permits end users of consumer reports to share the consumer report with another entity if Client and the other entity will use the report for the same transaction and for the same purpose. Examples include: a staffing company sharing a report with its customer with whom the consumer will be placed; a subcontractor sharing reports of its employees with the general contractor or owners of the project on which subcontractor is working. These examples are not exclusive, but demonstrate the acceptable "joint use" that is permitted. However, prior to sharing a consumer report, Client on behalf of AOA will determine and verify the identity of the joint user and that such joint user shares the same permissible purpose for use of the consumer report as does Client and the joint user will only use the consumer report for this one transaction with Client. Client shall obtain the consumer's authorization to share the report. This Agreement is a certification by Client that any joint user is a legitimate business and will use the report for the same permissible purpose Client represents to AOA when ordering the consumer report(s) on the individual consumer or as provided in Section 2 of this Agreement. **Client will need to make sure that the disclosure and authorization discloses and consents to such sharing.** Client agrees to indemnify and hold AOA harmless from any claims, liability or losses asserting that the joint use was improper in any way, violated the FCRA or otherwise, and additionally, if the joint user used the consumer reports for any reason than as represented by Client to AOA. Such indemnification includes all costs, expenses and reasonable attorney fees incurred by AOA.
C. Client represents that prior to requesting a report for **employment purposes (including contractors and volunteers)**, it will:
(i) disclose to the individual who is the subject of the report that a consumer report or, as applicable, an investigative consumer report, may be obtained;
(ii) obtain the written consent of the individual allowing the obtaining of the consumer report. Client agrees that submission of an order is a certification that it has obtained the consent of the consumer;
(iii) provide to the individual a summary of the individual's rights required under the ("FCRA") and any applicable state law;
(iv) obtain the written consent of the individual allowing the obtaining of the consumer report. Client agrees that the submission of an order is a certification that it has obtained the consent of the consumer;
(a) If client is a California employer, it agrees to include the following additional information in the disclosure and authorization/consent:
(i) Notice that an "investigative consumer report" as defined by California law, may be ordered regarding the consumer's character, general reputation, personal characteristics and mode of living,
(ii) AOA's name, address and toll-free telephone number,
(iii) The permissible purpose of the report,
(iv) The nature and scope of the investigation to be conducted,
(v) Notice that the consumer can request a copy of his/her file from us during normal business hours and the procedures for doing so,
(vi) A checkbox where the consumer may indicate he/she would like to receive a copy of the report,
D. Client further certifies that it will:
(i) not utilize any information in violation of any federal or state equal employment opportunity law or regulation.
(ii) not order criminal record information prior to the time permitted by applicable law, ordinance or regulation commonly referred to as "ban-the-box" restrictions.
(iii) provide a reasonable amount of time (recommend a minimum of 5 days) prior to taking adverse employment action against the individual who is the subject of the report, when such action will be based in whole or in part upon the information contained in the report furnished by AOA, the Client will, except as otherwise provided by law, advise the subject of the intent to take adverse action and provide a copy of the report to the individual and a description, in writing, of the individual's rights under the FCRA.
(iv) provide after taking adverse action based in whole or in part upon information contained in a report furnished by AOA, the Client shall:
(a) provide notice of such action to the individual;
(b) provide the name, address and telephone number of AOA; and
(c) inform the individual that he/she is entitled to a free copy of the report and a right to dispute the record through AOA and that AOA is unable to provide the individual the specific reasons why the adverse action was taken by you.
(v) comply with the FCRA and similar state laws, in regard to all reports, it will follow the requirements of the ("DPPA") and the various state laws implementing the DPPA in regard to motor vehicle reports.
E. Client represents that prior to requesting a report **for residential screening purposes**, it will:
(i) disclose to the individual who is the subject of the report that a consumer report or, as applicable, an investigative consumer report, may be obtained;
(ii) provide to the individual a summary of the individual's rights under the ("FCRA"); and
(iii) not utilize any information in violation of any federal, state or local equal housing law or regulation.
(iv) provide after taking adverse action e.g., rejecting, increasing rental rates, increasing deposit requirements, etc. against the subject of the report, based in whole or in part upon information contained in a report furnished by AOA, the Client shall:
(a) provide notice of such action to the individual;
(b) provide the name, address and telephone number of AOA;
(c) inform the individual that he/she is entitled to a free copy of the report and a right to dispute the record through AOA and that AOA is unable to provide the individual the specific reasons why the adverse action was taken by you; and
(d) providing a copy of the individual's rights under the FCRA.
F. Client represents that, if it orders credit reports, it will have a policy and procedures in place to investigate any discrepancy in a consumer's address when notified by the credit bureau that the consumer's address, as submitted by the client, substantially varies from the address the credit bureau has on file for that consumer. Further, if client hires the consumer and in the ordinary course of its business it furnishes information to the credit bureau from which the report came, that it will advise the credit bureau of the address it has verified as accurate if that address is different from the one provided by the credit bureau. If Client requests to receive credit reports the Parties will enter into an addendum adopting the requirements upon an end-user of the credit bureau's reports. Client acknowledges that AOA is not authorized to modify those terms.
G. Client will maintain documentation showing compliance with these certifications for a period of two (2) years or during the employment, tenancy, etc. of the subject, whichever is longer.

3. Compliance with Applicable Law

A. The laws relating to the furnishing and use of information are subject to change. It is the responsibility of Client to become knowledgeable in such laws and to comply with them. The failure to comply with the then current applicable law may result in a breach of this agreement, termination of service, civil and criminal liability. AOA does not undertake any obligation to advise Client of its legal obligations.
B. AOA does not act as legal counsel for Client. Client is responsible for retaining counsel to advise it regarding proper use of consumer reports; compliance with the FCRA, the Driver Privacy Protection Act, 18 U.S.C. §2721 et seq ("DPPA") and other applicable federal, state and local laws; and development of an appropriate screening program for Client's use of consumer reports.
C. Client agrees to promptly execute and return to AOA all documentation required, now or in the future, by any government agency or AOA to permit release of information or to ensure compliance with applicable laws or regulations. Such documentation shall become part of this agreement. The failure to return such documentation will result in Client being blocked from receiving the information related to the documentation, and, in some circumstances, all service may be terminated without additional notice.
D. Client consents to any reasonable request by AOA to audit records of the Client in person or by requesting copies of documents and to communicate with employees of the Client, with notice to Client, to determine the appropriateness of any present or past request(s) for information by Client. A failure to cooperate with an audit may result in the immediate termination or suspension of service.

4. Fees for Services

A. AOA will charge a fee for each request made by Client, in accordance with AOA's current fees schedule. AOA reserves the right to change the fees charged upon thirty (30) days notice to Client. Applicable sales or other taxes will be added to all fees. Client understands that AOA may incur access charges imposed by courts and other governmental agencies which are passed along to Client in addition to fees. These costs are subject to change without notice.
B. Payment on all invoices will be due thirty (30) days after billing. For any invoice not paid within thirty (30) days, AOA will add and collect a SERVICE CHARGE of one and a half percent (1½%) per month (or

the maximum permitted by applicable law, if lower) with a minimum service charge of $2. Client agrees to pay AOA's reasonable attorney's fees and costs incurred in enforcing the terms of this Agreement and in the collection of amounts due under this Agreement.

5. Confidentiality of Information

A. Information provided by AOA to its Clients is considered confidential by law. Upon its receipt, Client shall treat the information as confidential. Such information shall be maintained in confidential files to which access is restricted. Only those employees who need such information to perform their job duties shall have access to the same. Client shall ensure that such employees shall not attempt to obtain any consumer reports on themselves, family, friends or associates except in the exercise of their official duties. Client shall supply to AOA the name and phone number of the contact person or persons with whom AOA may discuss the contents of reports furnished to Client. At the time that Client disposes of any report received it shall cause such to be destroyed by cross shredding, burning or electronic destruction as required by regulations issued by the Federal Trade Commission. 16 CFR §682.1 et seq.

B. Client acknowledges that it will receive personal identifying information on the subjects of the reports it receives. Client shall maintain reasonable procedures to protect the information from unauthorized internal or external access. Within 30 days of the execution of this Agreement, Client will outline its protections in regard to the receipt, usage and storage of this information. Client shall, upon request, advise us of the status of Client's security measures. If Client experiences a breach of security regarding this information or discontinues any security measure, Client shall notify us within 24 business hours of the breach or discontinuance. With seven (7) business days of such an event, Client shall advise us what steps have been taken to protect the information from the reoccurrence of the breach or to restore protection of the information.

6. Waiver and Release

A. Client acknowledges that AOA relies totally on the information furnished by others. AOA also relies on the information contained in the records of various governmental agencies for other reports. AOA is not responsible for inaccurate or false information received from others and sent to Client. Client agrees to assert no claim and waives liability against AOA for any inaccurate or false information included in any report unless AOA had actual knowledge of the error and failed to correct it if it had the legal ability to alter such information.

B. Client agrees to hold AOA harmless and will indemnify AOA from all claims and losses resulting from Client's breach of this Agreement or violation of any applicable law. AOA agrees to hold Client harmless for all claims and losses arising from AOA's violation of any applicable law. Such indemnifications include all costs and reasonable attorney fees incurred by the indemnified party.

C. If the party seeking indemnification proposes to settle any claim it believes is subject to indemnification, it must notify the indemnifying party of such settlement and the indemnifying party must approve such settlement. Such approval shall not be unreasonably withheld. The indemnifying party can also disapprove of such settlement on the basis that the claim is not within those claims or losses covered by the indemnification. If the indemnifying party accepts the request to indemnify, but disagrees with the settlement amount, the indemnifying party shall take over the defense of the claim.

7. Misuse of Information

The FCRA prohibits the obtaining of information from a consumer reporting agency for an impermissible purpose. Further, those involved in such improper requesting may be subject to criminal penalties of imprisonment up to two years and/or a fine of $5,000 for each offense. 15 U.S.C. § 1681q. However such punishments are subject to change as the FCRA is amended. Further, the DPPA prohibits obtaining information under false pretenses and restricts the resale or redisclosure of personal information contained in state motor vehicle records. A violation of the DPPA may also result in criminal penalties. 18 U.S.C. § 2733(a). If a Client or one of its employees misrepresents to AOA the reason for a report or requests a report for an impermissible purpose, AOA may terminate service without notice in addition to other remedies available to AOA. Client understands that its misuse of or improper request for information may have a direct impact upon AOA and may cause it to be unable to obtain information for any of its clients resulting in substantial damages for which Client would be liable.

8. Non-Disclosure

Neither party shall, during the term of this Agreement, and any extension thereof and for reasonable time thereafter disclose to another or use, unless authorized by the disclosing party, any of the disclosing party's "Confidential Information". The purpose of this section, "Confidential Information" shall mean all the party's prospect list, client information, any customer records/information, employee list, financial data, business plans, business strategies, proprietary software and any other information of a party disclosed by one party to the other. Notwithstanding anything to the contrary contained in this Agreement, the receiving party shall not be precluded from: a) the use or disclosure of any Confidential Information which is currently known generally to the public or which subsequently has come into the public domain, other than by way of disclosure in violation of this Agreement; b) the use or disclosure of any Confidential Information that becomes available to the receiving party on a non-confidential basis from a source other than the disclosing party, provided that such source is not known by the receiving party to have a legal obligation prohibiting the disclosure of such information; or c) the use or disclosure of any Confidential Information that was developed independently by the receiving party, or d) the disclosure of the Confidential Information is required by law or legal process.

9. Termination of Agreement

A. Client may terminate this Agreement at any time upon written notice to AOA _. Client will remain liable for all charges made to its account prior to termination and will promptly pay all sums due on termination.

B. AOA may terminate this agreement by providing a sixty (60) day written notice but upon the occurrence of the following events, AOA may, immediately and without notice terminate or suspend this Service Agreement:

(i) Default in payment of charges for AOA Services;
(ii) Misuse of information contained in an AOA report;
(iii) Improper request for information;
(iv) Failure of Client to comply with or assist AOA in complying with the FCRA or any other applicable law;
(v) A material breach of this Agreement or violation of any law or regulation governing the request, use or release of the information in the reports by Client.
(vi) Unauthorized release of information in a consumer report to a third party or the reselling of any report.

10. Notice of Change in Client's Business

Client shall immediately notify AOA of any of the following events: change in ownership of the Client (over 50%); a merger, change in name or change in the nature of Client's business that in any way affects Client's right to request and receive consumer reports.

11. Miscellaneous Provisions

A. This Agreement constitutes the entire understanding between the parties and supersedes all previous agreements, negotiations and representations. This Agreement may only be modified in writing signed by both parties; however, subsequent representations by Client to show compliance with existing or future laws are effective when signed by Client and become a part of this Agreement. This Agreement is for the exclusive benefit of the parties hereto and no benefit is intended for any third party.

B. All communications and notices to be given under this Agreement will be made to the addresses, street and e-mail, and telephone numbers set forth herein. Each party will notify the other promptly of any change of address or telephone number.

C. This Agreement is intended to be subject to, and in compliance with, all applicable state and federal statutes and regulations. Insofar as this Agreement or any provision may subsequently be determined to be at variance or not in compliance with any such statute or regulation, it will be considered to be amended or modified to the extent necessary to make it comply, and AOA and Client hereby consent and agree to any such amendment or modification. Further, the invalidity of any one provision shall not affect the validity of the other provisions.

D. This Agreement is deemed to have become effective and to have been entered into upon its acceptance in the State of California by AOA. Therefore, this Agreement will be interpreted and enforced in accordance with the laws of the State of California, without reference to its conflict of laws, or any California law pre-empted by the FCRA.

E. AOA may make changes to the software or methods used to provide service to Client and Client must make any necessary changes to maintain working connection to the service at Client's sole cost.

12. Force Majeure

Both Parties are not responsible for any events or circumstances beyond its control that prevent it from meeting its obligations, which include but are not limited to: war, terrorism, riots, embargos, strikes, disruptions in communications or acts of God.

Signature	Membership Number	Date

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 is 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 algorithms 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 of 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 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 smartphones such as iPads, iPhones, Android based devices, etc.
3.6 When using smart tablets or smartphones 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 smartphones 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's 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, the 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 ongoing 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 _____ Membership Number _____ Date _____

RENTAL PROPERTY LIST

Property Address

Example: 1234 First St. Los Angeles CA, 90055

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

11. _____

12. _____

13. _____

14. _____

15. _____

16. _____

17. _____

18. _____

19. _____

20. _____

21. _____

22. _____

_____ _____ _____

Signature Membership Number Date