



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

SureDecision Packet

With identity theft on the rise, the credit bureaus have made it impossible for smaller landlords to obtain a full credit report and score on a rental applicant. Rather than focus on changes* in accessing credit bureaus as a hardship, we have used them to find an opportunity. These changes in policy have inspired us to help our clients that do not qualify to receive a full credit report.

In response, we have created *SureDecision*, a system that generates a “Pass, Conditional, or Fail” recommendation based on your applicant’s credit score. This gives you the ability to use the scoring information to assess your applicant’s credit health without seeing the actual credit bureau and score.

This simplified process takes away some of the confusion and complexities that come with a traditional credit report yet provides you with valuable, decision making information.

Please read and complete this packet in its entirety and send with required documents. Please see the “Required Documents” section for what is needed for your specific type of business. An account cannot be created until we have the documents needed. **Please send all pages in this packet including those that do not require writing or signing.**

There is a one time **\$35 setup fee. The turn around time for an account set up is no more than two business days once we have received all the required documents (see required documents section).** When you receive an e-mail with your username and password you will submit your background investigation(s) online.

The cost to run a credit and background investigation is **\$35 per person. Turn around time *once the background investigation is submitted* is about four to six business hours.** Some circumstances may require additional time.

Please contact our customer service department for questions. 480-305-1350 opt 2.

*In order to receive a copy of a credit bureau you must meet certain requirements, which include, **but are not limited to:**

1. Commercial building with a permanent sign (executive suites and home offices do not qualify)
2. Your company name and phone number published in the yellow pages for at least one year.
3. Locking cabinets in your office



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

Required Documents

There are certain documents needed before we issue an account. Please see the section that applies to you for what we need. An account cannot be created until we have the proper documents. In some cases more documentation may be requested. If you feel you do not fit into any of these categories please call our customer service department by dialing 480-305-1350 option 2. Please return this packet and the required documents by faxing to 480-668-7425 or e-mail orders@aaalandlord.com. *Please send all pages in this packet including those that do not require writing or signing.*

Landlord:

1. Proof of ownership of the rental property(ies) listed. Acceptable documents may include a copy of the filed property title, a copy of the property tax record, or property insurance documents.
2. A copy of a **completed and signed** rental application or agreement **for each property** (either an existing tenant or a new applicant is acceptable).
3. Copy of a phone bill **listed in the contact's name** (bill must show the phone number).

Real Estate Agent or Company:

1. Three **completed and signed** rental applications or agreements (either existing tenants or new applicants are acceptable).
2. Copy of phone bill **listed in the contact's name** or the company name (bill must show the phone number).

Apartment/Property Management Company:

1. Three **completed and signed** rental applications or agreements (either existing tenants or new applicants are acceptable).
2. Copy of phone bill **listed in contact's name** or the company name (bill must show the phone number).



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

CONTACT INFORMATION

All information will only be used to identify you as a landlord, property manager, realtor or business and is not used for any other purpose. All information will be kept private. Business names must be registered in your name and verifiable.

Client/Business name: _____

Type of business (Ex. landlord, realtor, property manager etc): _____

Client physical address: _____

City, state, zip code: _____

Contact person: _____ Year of birth _____

Business Phone: _____ Alt phone: _____

E-mail: _____ Fax: _____

RENTAL CREDIT: Based on your applicants FICO score, our system will generate a decision. Decisions will be as follows:

PASS- "Average Risk" Credit Score 600-825: Acceptable credit range for residential rental applicants.

CONDITIONAL- "Increased Risk" Credit Score 500-599: Credit range that requires additional deposits or co-signer prior to occupancy.

FAIL- "High Risk" Credit Score below 500: Unacceptable credit range for rental applicants.

AUTOMATICALLY DENIED FOR THE FOLLOWING

This will fail the application regardless of the credit rating if you check the corresponding box. Setting up criteria ahead of time is a way to stay consistent and will protect you as a landlord.

Criminal:

Evictions:

Felonies within (___) years

Unpaid evictions within (___) years

Violent misdemeanors within (___) years

Evictions within (___) years

Drug misdemeanors within (___) years

Rental collections within (___) years

DO NOT WRITE BELOW LINE-OFFICIAL USE ONLY

Username: _____ Password: _____



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

LIST OF PROPERTIES

Please list all the rental properties you will be screening for and sign the page. Under property name please list the name the property is under for tax purposes. Please include one rental application for each rental property as part of the required documents (see page 2).

Property Name	Property Address	City, State, Zip
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Signature/Title

Date



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

Credit Card Authorization

CREDIT CARDHOLDER INFORMATION			
NAME ON CREDIT CARD			
TYPE OF CREDIT CARD	VISA	DISCOVER	MASTERCARD
TYPE OF ACCOUNT	PERSONAL		BUSINESS
COMPANY NAME			

ACCOUNT NUMBER					
EXPIRATION DATE					
BILLING ADDRESS					
CITY		STATE		ZIP CODE	
PHONE		EMAIL		FAX NUMBER	

AUTHORIZED USER OF CREDIT CARD	
NAME	
COMPANY	
PHONE NUMBER	
EMAIL ADDRESS	
IDENTIFICATION	
RELATION TO OWNER	

AUTHORIZATION OF CARD USE
<p>I certify that I am the authorized holder and signer of the credit card referenced above.</p> <p>I certify that all information above is complete and accurate.</p> <p>I hereby authorize collection of payment for all charges immediately upon order. Each order with Investigative will be charged separately.</p> <p>I hereby authorize a one time setup fee of \$35 to be charged to my credit card.</p>

CARDHOLDER NAME			
SIGNATURE		DATE	



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

Access Security Requirements

We must work together to protect the privacy and information of consumers. The following information security measures are designed to reduce unauthorized access to consumer information. It is your responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to employ an outside service provider to assist you. Capitalized terms used herein have the meaning given in the Glossary attached hereto. The credit reporting agency reserves the right to make changes to Access Security Requirements without notification. The information provided herewith provides minimum baselines for information security.

In accessing the credit reporting agency's services, you agree to follow these security requirements:

1. Implement Strong Access Control Measures

- 1.1 Do not provide your credit reporting agency Subscriber Codes or passwords to anyone. No one from the credit reporting agency will ever contact you and request your Subscriber Code number or password.
- 1.2 Proprietary or third party system access software must have credit reporting agency Subscriber Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.
- 1.3 You must request your Subscriber Code password be changed immediately when:
 - any system access software is replaced by system access software or is no longer used;
 - the hardware on which the software resides is upgraded, changed or disposed of
- 1.4 Protect credit reporting agency Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).
- 1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.
- 1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 1.7 Keep user passwords Confidential.
- 1.8 Develop strong passwords that are:
 - Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
 - Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to credit information.
- 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 your membership application.
- 1.13 Ensure that you and your employees do not access your 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.
- 1.14 Implement a process to terminate access rights immediately for users who access credit reporting agency 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.



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

- 1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.
- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

2. Maintain a Vulnerability Management Program

- 2.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- 2.2 Configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
- 2.3 Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
 - Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
 - If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
 - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
- 2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
 - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
 - If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
 - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
 - Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

3. Protect Data

- 3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)
- 3.2 All credit reporting agency data is classified as Confidential and must be secured to this requirement at a minimum
- 3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- 3.4 Encrypt all credit reporting agency data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- 3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

4. Maintain an Information Security Policy

- 4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- 4.2 Establish processes and procedures for responding to security violations, unusual or



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

- suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.
- 4.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

5. Build and Maintain a Secure Network

- 5.1 Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.
- 5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
- 5.3 Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.
- 5.4 Any stand alone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services and network traffic.
- 5.5 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

6. Regularly Monitor and Test Networks

- 6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 6.2 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access credit reporting agency 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.

Record Retention: *The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, the credit reporting agency 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 breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.*

“Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than \$2,500 per violation.”

Signature/Title

Date



INVESTIGATIVE

screening & consulting

A Division of AAA Tenant Screening, Inc.

FCRA Requirements

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

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. We have included a copy of the FCRA with your membership kit. We suggest that you and your employees become familiar with the following sections in particular*:

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

Each of these sections is of direct consequence to users who obtain reports on consumers. We strongly endorse the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce.

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

We support consumer reporting legislation that will assure fair and equitable treatment for all consumers and users of credit information.

I acknowledge my responsibilities under the FCRA. I also acknowledge my responsibilities for access security. I will not further sell the information received from the consumer report. I attest that all of the above information is correct and accurate. Any reports provided by AAA Tenant Screening I will use for rental purposes only. I will receive a signature with authorization to pull credit from all of my applicants.

Signature/Title

Date

*To review the above sections of the FCRA go to <http://www.ftc.gov/os/statutes/fcradoc.pdf>