

## Membership Application

Membership Name: \_\_\_\_\_ Number of rental units: \_\_\_\_\_

Authentication code: \_\_\_\_\_ How did you hear of us? \_\_\_\_\_

Member is a (Check one):  Individual Owner/Landlord  Property Management Company  Re-Seller

Organization structure (Check one):  Corporation  Proprietorship  Joint Venture  LLC  Partnership

Member operates business from a:  Commercial Building  Private Residence

Address: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

Phone Number: (\_\_\_\_\_) \_\_\_\_\_ Fax Number: (\_\_\_\_\_) \_\_\_\_\_

Main contact name: First: \_\_\_\_\_ Last: \_\_\_\_\_

Position/Title: \_\_\_\_\_ Company Web Site: \_\_\_\_\_

### Address of rental property (if more than one property, please attach a property list)

Address: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

### Check if billing contact is the same as above

Billing contact name: First: \_\_\_\_\_ Last: \_\_\_\_\_

Address: \_\_\_\_\_ State: \_\_\_\_\_ Zip: \_\_\_\_\_

Phone Number: (\_\_\_\_\_) \_\_\_\_\_ Fax Number: (\_\_\_\_\_) \_\_\_\_\_

Position/Title: \_\_\_\_\_ Email: \_\_\_\_\_

### Personal Guarantor

Individual who personally guarantees payment of charges: First: \_\_\_\_\_ Last: \_\_\_\_\_

Social Security Number: \_\_\_\_\_ Residence address: \_\_\_\_\_

(Guarantor/Member understands by the signature below, that The Screening Pros, LLC may pull a personal credit report in connection with the approval of this application for membership)

### Lawful Usage

Is member licensed to do business as, or providing services to an attorney or private investigation agency?  Yes  No

Does the member intend to resell or release information from the consumer credit report to a third party?  Yes  No

Will member provide credit repair or credit counseling services for a fee?  Yes  No

Member understands that obtaining confidential consumer credit reports other than for the purposes set forth by legitimate business purposes established by The Fair Credit Reporting Act and specific state and federal laws is a crime and punishable by imprisonment. Member agrees to pay The Screening Pros, LLC. (TSP) in full all incurred charges rendered during the previous billing period upon receipt of monthly statement. Member agrees to pay a late fee of 1.5% per month on all charges that are past due. Member agrees to defend and hold TSP harmless in the event that member, member's employees and/or agents violate the law. Member agrees to pay a non-refundable application processing fee of \$118.00 which is due upon submittal of the completed membership application.

Member's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

## Service Agreement

As a Consumer Reporting Agency (CRA), state and federal law requires that The Screening Pros, LLC (TSP) investigates those applying for membership as well as to regularly validate through continued investigation a member's legitimate business need for consumer credit reports. As a CRA defined under the laws of the Fair Credit Reporting Act (FCRA) sec. 604 (15 USC 1681b) and in some cases, more stringent state laws, It is the responsibility of TSP to verify that the applicant for membership has a legitimate permissible purpose for obtaining consumer credit reports and supplies TSP with the required compliance documentation required by the credit bureaus to validate the legitimate need for confidential consumer credit data.

Compliance documentation required in establishing membership with TSP as mentioned above is as follows:

- A copy of member's telephone bill or listing in phone book.
- Three (3) signed rental applications.
- Proof of ownership of your rental property showing the same name as the applying membership name. Such as a tax bill or property deed dated within the past twelve (12) months.
- Three business trade references.
- Signed and dated list of properties you own and/or manage.
- Front page of applying member's bank statement with account balance, name and account number.
- Letter of intent stating the nature of your business and intended use for the service.
- An on-site inspection performed either by an agent of The Screening Pros, LLC or a third party inspection company. (Third Party Inspection Company required to obtain Experian credit reports and additional inspection fees would apply and be paid by member)

\*If member manages rental property for other owners for a fee, you must also supply the following:

- A copy of one contract between the management company and a representative property owner for whom the management company manages property.

1. Reseller (TSP) has access to consumer reports from one or more consumer reporting agencies.
2. Member acknowledges their responsibilities of obtaining confidential consumer credit reports as defined by Section 604 of the FCRA (15 USC 1681b) as amended by the Consumer Credit Reporting Reform Act of 1996, hereinafter called "FCRA." The subscriber certifies their permissible purpose as:

Extension of credit and/or review of credit account     Collection of an account or judgment

Employment Purposes     Residential/Commercial rental purposes

3. Member certifies that they will request consumer reports pursuant to procedures prescribed by TSP solely for the permissible purpose certified above, and will use the reports obtained for no other purpose.
4. Member will maintain copies of all written authorizations, consumer application and consumer reports for a minimum of three (3) years from the date of inquiry.
5. THE FCRA PROVIDES THAT ANY PERSON WHO KNOWINGLY AND WILLFULLY OBTAINS INFORMATION ON A CONSUMER FROM A CONSUMER REPORTING AGENCY UNDER FALSE PRETENSES SHALL BE FINED UNDER TITLE 18, OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.

6. Member shall use each consumer report only for a one-time use and hold the report in strict confidence, and not to disclose it to any third parties.
7. Member will not re-sell any consumer reports and agree to all Internet access security guidelines.
8. With just cause, such as delinquency or violation of the terms of this contract or a legal requirement, or a material change in existing legal requirements which adversely affects this Agreement, Reseller (TSP) may, upon its election, discontinue serving the Subscriber (member) and cancel this Agreement immediately.

Member's Signature: \_\_\_\_\_ Printed Name: \_\_\_\_\_

Title/Position: \_\_\_\_\_ Date: \_\_\_\_\_

Business References

1) Business Name: \_\_\_\_\_ Bus. Phone \_\_\_\_\_

Contact Name: \_\_\_\_\_ Type Of business: \_\_\_\_\_

2) Business Name: \_\_\_\_\_ Bus. Phone \_\_\_\_\_

Contact Name: \_\_\_\_\_ Type Of business: \_\_\_\_\_

3) Business Name: \_\_\_\_\_ Bus. Phone \_\_\_\_\_

Contact Name: \_\_\_\_\_ Type Of business: \_\_\_\_\_

4) Business Name: \_\_\_\_\_ Bus. Phone \_\_\_\_\_

Contact Name: \_\_\_\_\_ Type Of business: \_\_\_\_\_

5) Business Name: \_\_\_\_\_ Bus. Phone \_\_\_\_\_

Contact Name: \_\_\_\_\_ Type Of business: \_\_\_\_\_

## **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. 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.
- 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 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