



We're excited to work with you!

To ensure that we meet the high compliance standards required by the consumer reporting industry, some documentation is mandatory for our files in order to allow access to criminal background and credit reports for the purpose of tenant screening.

Let's get started!



Items to Submit for Account Activation:

- _ Business or real estate license in company name (If business, not required for landlords)
- _ Service Application (attached)
- _ Service Agreement (attached)
- _ Exhibit A – Required Terms (attached)
- _ Site Inspection Form (attached)
- _ Letter of Intent (attached)

Please fax all documents to us at 877-349-2175

Please note: Upon review of your documents, and per the requirements of the FCRA and the consumer reporting agencies, StarPoint Screening may request additional documentation and assurances before, during or after you have established service with us.

Thank you for choosing to work with StarPoint Screening!



Please Fill Out Your Account Information

Service Application

Account Information

Account's Billing Information

Check if same as Account Information [checkbox]

COMPANY NAME OR NAME OF LANDLORD (including all DBAs)

COMPANY NAME OR NAME OF LANDLORD

COMPANY ADDRESS OR LANDLORD ADDRESS (For above business entity)

COMPANY ADDRESS OR LANDLORD ADDRESS (For above business entity)

CITY STATE ZIP

CITY STATE ZIP

TELEPHONE FAX

YOUR FIRST NAME / MI / LAST NAME

E-MAIL ADDRESS

TELEPHONE FAX

YOUR FIRST NAME / MI / LAST NAME

E-MAIL ADDRESS

ADDITIONAL CONTACT PERSON

ADDITIONAL CONTACT PERSON

NAME OF PRINCIPAL/OWNER (if different than yourself)

SOCIAL SECURITY NUMBER OF PRINCIPAL/OWNER

FED TAX ID NUMBER OF BUSINESS ENTITY (If applicable)

BUSINESS TYPE: SOLE PROPRIETOR, PARTNERSHIP, CORPORATION, LANDLORD

YEARS ESTABLISHED

NATURE OF BUSINESS (Landlord, Property Management, Realty Office, etc)

COMPANY OR LANDLORD WEBSITE/URLS (if applicable)



Service Agreement

THIS AGREEMENT is made on _____, 20____,

between _____ ("End User") and StarPoint Screening ("StarPoint").

1. This Agreement states the terms and conditions under which StarPoint Screening will provide consumer credit reports to End User.
2. When requested by End User, StarPoint Screening will provide End User with consumer credit reports ("Reports") after a request from End User.
 - a. End User agrees to make full payment within fifteen (15) days after the date of each invoice from StarPoint. Past due amounts will be subject to a late charge of the greater of \$15 or 1.5% of the past due amount and, in addition, will bear interest at the rate of twenty-four percent (24%) per annum, beginning on the date of invoice and continuing until paid.
 - b. End User understands that StarPoint Screening provides Reports prepared and compiled by others and, for that reason, StarPoint Screening cannot and does not guarantee the accuracy of any Report. End User releases StarPoint Screening from all claims, liabilities, costs and expenses of every kind and nature relating in any way to inaccurate or incomplete information in any Report.
3. This Agreement is effective when (i) StarPoint Screening receives from End User all documents StarPoint Screening requires to open the account and (ii) StarPoint Screening activates End User's account. After this Agreement becomes effective, it will continue in full force and effect until terminated by either End User or StarPoint.
4. End User and StarPoint Screening each agrees that it will at all times fully comply with the Federal Fair Credit Reporting Act, and all other applicable state, federal and local laws and regulations. Without limitation, End User will at all times fully comply with the requirements set forth in Exhibit A in this Agreement.
5. End User recognizes that it has a joint responsibility with STARPOINT SCREENING to protect the privacy of consumers, as set forth in Exhibit B to this Agreement.
6. This Agreement and the relationship between End User and StarPoint Screening (to the extent not specified in this Agreement) will be governed by the Uniform Commercial Code as most currently adopted by both the American Law Institute and the National Conference of Commissioners on Uniform State Laws.
7. End User does not have the right or ability to assign any or all of its rights under this Agreement. Any change in ownership of a majority of End User's equity will be considered a prohibited assignment of End User's rights under this Agreement.
8. To the extent any provision of the California Civil Code applies to any Report requested by End User, End User agrees that it will be responsible for full compliance with all applicable requirements of the California Civil Code, and that StarPoint Screening will have no such responsibility.
9. If there is any litigation or arbitration proceeding between End User and StarPoint, whether relating to this Agreement or otherwise, in addition to all other appropriate relief, the prevailing party will be entitled to recover its attorneys' fees and other costs incurred in the proceedings.

PLEASE FAX THIS FORM TO US AT 877-349-2175

10. This Agreement sets forth the parties' entire understanding with respect to the subject matter hereof and, in regard to its subject matter, this Agreement supersedes all prior letters of intent, agreements, arrangements, communications, representations, and warranties, whether oral or written, by any officer, employee, or representative of either party.

11. END USER AGREES THAT IN NO EVENT SHALL STARPOINT SCREENING BE LIABLE UNDER ANY THEORY OF LIABILITY (INCLUDING, BUT NOT LIMITED TO, BREACH OF CONTRACT, BREACH OF WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER THEORY OF LIABILITY) FOR (A) DIRECT DAMAGES OR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES SUCH AS, BUT NOT LIMITED TO, DOWNTIME, INTERRUPTION IN USE, UNAVAILABILITY OF PRODUCT OR SERVICE, LOSS OF INFORMATION OR DATA, LOST PROFITS, EXEMPLARY OR PUNITIVE DAMAGES, OR ANY OTHER DAMAGES, WHETHER OR NOT FORESEEABLE AND WHETHER OR NOT STARPOINT SCREENING OR ITS REPRESENTATIVES OR AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR (B) ANY OTHER CLAIM, DEMAND OR DAMAGES OF ANY KIND OR NATURE RESULTING FROM OR ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR THE DELIVERY, USE OR PERFORMANCE OF STARPOINT'S PRODUCTS AND SERVICES. THIS LIMITATION OF LIABILITY ALSO EXTENDS TO ANY SUPPLIER OR LICENSOR OF ALL OR ANY PART OF STARPOINT'S PRODUCTS AND SERVICES. EACH SUCH SUPPLIER OR LICENSOR IS AN INTENDED BENEFICIARY OF THIS LIMITATION OF LIABILITY.

Signature: _____ Title : _____

Name: _____

PLEASE FAX THIS FORM TO US AT 877-349-2175



Exhibit A - Required Terms

Required Terms for Agreement Between Reseller and User for Consumer Reports

End User is a _____ [insert type of business] and has a permissible purpose for obtaining consumer reports in accordance with the Fair Credit Reporting Act (15 U.S.C. §1681 et seq.) including, without limitation, all amendments thereto ("FCRA"). The End User certifies its permissible purpose as:

1.

- In connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of credit to, or review or collection of an account of the consumer; or
- In connection with the underwriting of insurance involving the consumer or review of existing policy holders for insurance underwriting purposes, or in connection with an insurance claim where written permission of the consumer has been obtained; or
- In connection with a tenant screening application involving the consumer; or
- In accordance with the written instructions of the consumer; or
- For a legitimate business need in connection with a business transaction that is initiated by the consumer; or
- As a potential investor, servicer or current insurer in connection with a valuation of, or assessment of, the credit or prepayment risks.

→
Please pick the box that explains the purpose for which are pulling credit reports

2. End User certifies that End User shall use the consumer reports: (a) solely for the Subscriber's certified use(s); and (b) solely for End User's exclusive one-time use. End User shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with End User's own data, or otherwise in any service which is derived from the consumer reports. The consumer reports shall be requested by, and disclosed by End User only to End User's designated and authorized employees having a need to know and only to the extent necessary to enable End User to use the Consumer Reports in accordance with this Agreement. End User shall ensure that such designated and authorized employees shall not attempt to obtain any Consumer Reports on themselves, associates, or any other person except in the exercise of their official duties.
3. End User will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.
4. 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 OF THE UNITED STATES CODE OR IMPRISONED NOT MORE THAN TWO YEARS, OR BOTH.
5. End User shall use each Consumer Report only for a one-time use and shall hold the report in strict confidence, and not disclose it to any third parties; provided, however, that End User may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, unless otherwise explicitly authorized in an agreement between Reseller and its End User for scores obtained from TransUnion, or as explicitly otherwise authorized in advance and in writing by TransUnion through Reseller, End User shall not disclose to consumers or any third party, any or all such scores provided under such agreement, unless clearly required by law.

6. With just cause, such as violation of the terms of the End User's contract or a legal requirement, or a material change in existing legal requirements that adversely affects the End User's agreement, Reseller may, upon its election, discontinue serving the End User and cancel the agreement immediately.

For those End Users that wish to receive TransUnion Scores as part of the consumer credit report being delivered, the agreement between Reseller and End User must also contain the following language:

1. End User will request Scores only for End User's exclusive use. End User may store Scores solely for End User's own use in furtherance of End User's original purpose for obtaining the Scores. End User shall not use the Scores for model development or model calibration and shall not reverse engineer the Score. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any Person except (i) to those employees of End User with a need to know and in the course of their employment; (ii) to those third party processing agents of End User who have executed an agreement that limits the use of the Scores by the third party to the use permitted to End User and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; or (iv) as required by law.

Signature: _____ Title : _____

Name: _____

PLEASE FAX THIS FORM TO US AT 877-349-2175



Site Inspection Form

The "Site" is the location where you will order and access the credit reports (your office or your home).

Company Name or Landlord Name: _____

Main Contact on Account: _____

Landlord or Company's Physical Address: _____

1. Is the company or landlord located at the exact address provided on the membership application? If not, please explain: _____ Yes No
2. Is the company or landlord working out of their home? Yes No
- 2a. If yes, is the home office in a separate room from the living area? Yes No NA
3. Are you involved in or associated with credit repair, brokering, reselling or releasing credit reports or investigative, detective, private investigative, legal or law enforcement services? Yes No
4. Is the computer used to access or request credit reports password protected? Yes No
5. Is there a locking door for the premises where credit reports are accessed and stored? Yes No
6. Is there a locking filing cabinet or desk where any printed credit reports can be stored? Yes No
7. Is there a shredder to destroy any printed credit reports? Yes No
8. Is there a permanent exterior sign (For commercial offices only) Yes No NA

Third party filling out inspection: *I certify by signature below, that the findings of this inspection are accurate.*

(The third party may be a person from an adjacent business, a vendor that frequents your office or home office, a neighbor, etc.)

Third Party's Printed Name: _____ Signature: _____

Date: _____

StarPoint Applicant: *I certify by signature below, that the findings of this inspection are accurate.*

Signature: _____ Position/Title: _____

Print Name: _____ Date: _____

Please fax to us at 877-349-2175

Letter of Intent

Date: _____

To StarPoint Screening,

My interest in pulling Trans Union credit reports is to evaluate and screen the credit risk of prospective
_____ and for no other purpose.

Signature:

Printed Name:

Exhibit B- Access Security

End User will comply with STARPOINT SCREENING policies and procedures, which End User hereby acknowledges have been received and reviewed. End User will comply with additional, updated, or new requirements when received from STARPOINT SCREENING. End User recognizes that it has a joint responsibility with STARPOINT SCREENING to protect the privacy of consumers. The following measures are designed to reduce unauthorized access of consumer reports. In signing this Agreement, End User agrees to the following measures: To protect its STARPOINT SCREENING account number, user name, and password so that only key personnel know this sensitive information. Unauthorized persons should never have knowledge of such password. End User agrees not to post the information in any manner within its facility.

1. Assign each employee-user in its office his/her own unique user name and password. Do not allow employees to share login information.
 2. Do not divulge the STARPOINT SCREENING account number and passwords by telephone with any unknown caller.
 3. Restrict the ability to obtain consumer information to a few key personnel.
 4. Place all terminal devices / computers used to obtain consumer information in a secure location within its facility. End User should secure this equipment so that unauthorized persons cannot easily access it.
 5. After normal business hours, be sure to turn off and secure all systems used to obtain credit information.
 6. Secure hard copies and electronic files of consumer reports within End User's facility so that unauthorized persons cannot easily access them.
 7. Shred or destroy all hard copy consumer reports when no longer needed. Erase or scramble electronic files containing consumer information when no longer needed and when applicable regulation(s) permit destruction.
 8. E-mailing consumer data is prohibited. E-mail is not a secure method of data transfer, and should not be used to transmit sensitive material such as the contents of a consumer report.
 9. Make all employees aware that the company can access consumer information ONLY for the permissible purposes listed in the permissible purpose information section of your service application. End User employees may not access their own report or the report of a family member or friend if End User does not have permissible purpose.
- 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 United States Code, imprisoned for not more than two years, or both."** End User agrees to comply with all requirements of the FCRA and all other applicable laws in ordering and using credit reports.

Access Security Requirements

We must work together to protect the private information of consumers. These 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, you may employ an outside service provider to assist you. Capitalized terms used have the meaning given in the Glossary section. We reserve the right to change these Security Requirements. This information provides minimum baselines for information security.

In accessing the credit reporting services, the following security requirements apply:

1. Implement Strong Access Control Measures

- 1.1. Do not provide your Subscriber Codes or passwords to anyone. No one from our company will ever contact you and request your Subscriber Code number or password.
- 1.2. Proprietary or third party system access software must have the 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 their system access software or is no longer used; or the hardware on which the software resides is upgraded, changed or disposed of.
- 1.4. Protect 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 our system. 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 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) and that contain a minimum of eight (8) 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 your Contract.
- 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.

THIS PAGE IS FOR YOUR RECORDS ONLY

1.14. Implement a process to terminate access rights immediately for users who access credit reporting 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. • 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 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 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 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 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, you are required to 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, we 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.

THIS PAGE IS FOR YOUR RECORDS ONLY