Date of Application: _____

Check-Point | Membership Application

3539 Bradshaw Rd #307, Sacramento, CA 95827 | **Phone**: 888-534-1233 or 916-855-5472 | **Fax**: 888-332-4128 or 916-363-0977

info@checkpointscreening.com | www.checkpointscreening.com

I understand that the information provided below may be used to obtain a consumer credit report, and my creditworthiness may be considered when making a decision to grant access.

Owner / Property Management Company Information

Owner/Management Co Name:	# of Properties:
Physical Address:	
Phone:	Fax:
Email:	Website:
Is this a residential address? ☐ Yes ☐ No	
Type of Ownership: ☐ Individual ☐ Partnership ☐ Nonprofit ☐ Corporation ☐ LLC ☐ Receiver	
Tax ID (or SSN if Individual):	
Nature of Business:	

Principle of the Company | complete if partnership

I understand that the information provided below may be used to obtain a consumer credit report, and my creditworthiness may be considered when making a decision to grant membership.

Principle Name:	Title or Position:
Social Security Number:	Date of Birth:
Residential Address:	

Property Information (For Multiple Properties, Please Submit Separate List):

Property Name:	# of Units:
Resident Manager:	
Type of Units: (check all that apply) ☐ SFR ☐ Multi-Unit ☐ Section 8/HUD ☐ Commercial ☐ Other	
Property Address:	

Phone:	Fax:	Email:

Billing Information

Send Bills to: ☐ Property Address ☐ Owner/Mgmt. Co Address ☐ Other:	
Billing Contact:	Phone:
Billing Email:	

Sales Rep: _____ Client Code: _____

Permissible Purpose | application will not be processed without this information

Estimated number of reports processed monthly:

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

Do you have an Investigative License? ☐ **Yes** ☐ **No** If yes, please provide a copy with this application.

Please choose which type of report you'll be running: ☐ decision only (evaluation - without credit) ☐ full credit (site inspection required)

Authorization Form

Would you like to authorize an agent to sign CheckPoint's User Agreement on your behalf? ☐ Yes ☐ No

I, _____ , authorize my agent _____

to complete and sign CheckPoint's User Agreement on my behalf.

Additional persons authorized to request reports under this account:

1. _____ 2. _____

3. _____ 4. _____

Signature: Date:

Terms of Use Agreement

CHECK-POINT.COM, LLC, (hereinafter "CP") is requested to establish one consumer credit inquiry access account at the fee of $0. Subscriber is fully responsible for all charges made using the access codes relating to account regardless of whom actually makes the inquiries. In the event of unauthorized use or departure of authorized employees, subscriber must notify CP immediately and CP will then change the access code. Report process is subject to change by CP and may be changed at any time subject to 10 days notice to customer. All amounts charged on this account are subject to an interest rate of 18% PA until fully paid. Any account that is 30 days or more past due may be denied access. A Late charge of five percent of the invoice amount or $ 20.00 whichever is the greater, may be applied if any payment is not made within terms. In the event of any default or improper use of the credit information obtained under this account, the subscriber agrees to pay reasonable attorney fees and court costs and to hold CP harmless of all damages, costs, claims judgments against CP including applicable attorney's fees. Exclusive venue for any court action under this agreement will be Sacramento, California. CP and the credit data Repositories from which we draw information endeavors to provide the most accurate and verified data possible, but neither guarantees the accuracy of any data provided and neither shall be liable for actual and/or consequential damages occurring as a result of providing erroneous or improper data to subscriber. Subscriber hereby certifies and agrees: That it will request and use credit information received from CP solely in connection with bona fide credit or rental transactions, or for employment purposes, and will not request or use such information for any purposes not specifically authorized by applicable State or Federal laws including but not limited to 15 USC 1681 et seq. "Fair Credit Reporting Act" (hereinafter "laws"). Subscriber shall observe any additional requirement imposed by any credit repository that may be notified from time to time. Subscriber agrees to comply with all provisions of the LAWS. All credit information obtained hereunder shall be maintained by Customer in strict confidence and disclosed only as provided by law. The FCRA (Fair Credit Reporting Act) mandates that a physical inspection be conducted at the location where credit reports are stored. End-user is responsible for fees associated with inspection, until first months usage has been evaluated to determine waiver. **Subscriber will not sell or otherwise distribute to third party any information received hereunder, except to consumers as required by law. Subscriber agrees to abide by security requirements as outlined in "Usage Requirements."**

☐ I have read and understand the terms contained in the Check Point Agreement (listed above)

☐ I certify that I will use the CheckPoint product information for no other purpose other than what is stated in the **Permissible Purpose** section on this application and for the type of business listed on this application.

Company Name

Type or Print Name of Owner or Officer Title

Authorized Signature Date

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.

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.

7. Usage Requirements

7.1 If you are a **landlord**, a clear disclosure has been made in writing to the consumer at anytime before the reports is procured and that a consumer report be obtained for landlord purposes AND the consumer has authorized in writing the procurement of the report and provided a valid picture ID.
7.2 **Criminal Reports** – database criminal searches may be at least 120 days old at any given time. In California the most comprehensive criminal database contains only 14 counties. Additionally you have been provided an option to purchase a court runner that provides the most comprehensive and up-to date information within 48 hours. The Court Runner Criminal search is a standard 7 year search.

7.3 For Online Clients: **Please comply with the following security measures:**

• You must protect your User ID number and password so that only you know this sensitive information. Unauthorized persons should never have knowledge of your password. Do not post the information in any manner within your facility.

• Do not discuss your account number, User ID, and password by telephone with anyone even if caller claims to be a representative or employee of Consumer Credit Agency.
• Restrict ability to obtain/view credit reports to a few key personnel.
• Check-Point must be notified immediately when a staff member with access to online reports leaves your company.
• Place all terminal devices used to obtain credit information in a secure location within your facility. You should secure these devices so that unauthorized persons cannot easily access them.
• After normal business hours, be sure to turn off and lock devices or systems used to obtain/view credit information.
• Secure hard copies and electronic files of consumer reports within your facility so that unauthorized persons cannot easily access them.
• Shred or destroy all hard copy of 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.
• Make all employees aware that your company can access credit information only for the permissible purpose of your membership. Your employees may not access their own report or the report of a family member or friend.
• By agreeing to this document you agree to release Check-Point and the Credit Repositories from any litigation, damages, and liabilities arising from supplying/printing/viewing credit reports. You further agree to comply with the FCRA and this Access Security Service Agreement in its entirety.

7.4 ***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."

8. FCRA Requirements
Federal Fair Credit Reporting Act *(as amended by the Consumer Credit Reporting Reform Act of 1996)*

8.1 Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. You can review a copy of the FCRA at http://www.ftc.gov/os/statutes/fcrajump.htm. We suggest that you and your employees become familiar with the following sections in particular:

- **§ 604. Permissible Purposes of Reports**
- **§ 607. Compliance Procedures**
- **§ 610. Conditions and Form of Disclosure to Consumers**
- **§ 611. Procedure in Case of Disputed Accuracy**
- **§ 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**
- **§ 620. Unauthorized Disclosures by Officers or Employees**
- **§ 621. Administrative Enforcement**
- **§ 623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies**

Each of these sections is of direct consequence to users who obtain reports on consumers.

8.2 As directed by the law, credit reports may be issued only if they are to be used for extending credit, review or collection of an account, employment purposes, underwriting insurance or in connection with some other legitimate business transaction such as in investment, partnership, etc. It is imperative that you identify each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact your usage of reports for employment purposes.

8.3 Experian strongly endorses the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce.

8.4 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 statues *and the statues and regulation of the states in which you operate.*

8.5 **Check-Point supports consumer reporting legislation that will assure fair and equitable treatment for all consumers and users of credit information.**

9. FICO Score Addendum

For End Users that are receiving FICO scores with the consumer report:

9.1 End User will request Scores only for End User's exclusive use under the FCRA "permissible purpose" state in the application;

9.2 End User's agreement 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;

9.3 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;

9.4 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 tenant screening or employee screening transactions and decisions only.

9.5 A requirement that each User comply with all applicable laws and regulations in using the Scores and reason codes purchased from Check Point.

9.6 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 Check Point.Com, LLC, or the affiliates, or of any other party involved in the scoring model development without such entity's prior written consent;

9.7 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 three credit bureaus in performing the scoring model.

9.8 Check-Point. Com, LLC assurances that the credit score Model used by the three major credit bureaus is empirically derived and demonstrably and statistically sound and that to the extend the population to which the Model is applied is similar to the population sample on which the Model was developed, the Model score may be relied upon by End Users to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to End Users. Check-Point, LLC further assures that so long as it provides the ability to obtain a score derived through the score Model, it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act, 15 USC Section 1691 *et seq.* THE FORGOING ASSURANCES ARE THE ONLY ASSURANCES CHECK-POINT.COM, LLC MIGHT HVE GIVEN END USERS WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, ASSURANCES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. End User's rights under the forgoing Assurance are expressly conditioned upon each respective End User's periodic revalidation of the credit score Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 *et seq.*).

9.9 In consideration of Check-Point.Com, LLC providing ability to obtain credit score based on Credit Score Model, End User will pay Check-Point.Com fees as agreed in the Price Agreement. A provision limiting the aggregate liability of Check-Point.Com, LLC to each End User for the Credit Score obtained 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 Resale Contract during six (6) month period, and excluding any liability of Check-Point.Com, LLC for incidental, indirect, special or consequential damages of any kind.

10. <u>Onsite Inspection</u>

10.1 If the end user is located in a commercial area and applies to obtain a full credit report on consumers, they will be required to undergo a one-time physical inspection **or** if the end user is operating from a residential location and applies to obtain a full credit report on consumers, they will be required to undergo an annual physical inspection.

The following applies to users of consumer information products:

I have read and understand the attached "FCRA Requirements" notice and "Access Security Requirements" and will take all reasonable measures to enforce them within my facility. I certify that I will use the consumer information for no other purpose other than what is stated in the Permissible Purpose/Appropriate Use section on this application 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, the below signed and "End User", hereby certify that all information provided by myself, my company and/or my authorized users, is true and accurate. I understand and acknowledge that providing false information in this agreement can result in civil and federal consequences.

Company Name

Type or Print Name of Owner or Officer

Title

Authorized Signature

Date

In order to complete the account set-up and meet the requirements of the Fair Credit Reporting Act the following documents must be provided:

- **Copy of Your Photo ID**
- **Proof of Ownership for each Rental Property** *(title, tax record, insurance docs, deed, etc.)*
- **One Signed Rental Application** *(current or previous applicant)*
- **Copy of Telephone Bill** *(which shows your name, phone number and address)*

Please print and sign this application and fax it to CheckPoint along with copies of the above documents.

Fax: 888-332-4128

Please feel free to contact us if you have any questions regarding the Membership Application or other documents required for compliance. We are more than happy to assist you, and may be able to get your account set up as early as today.

Thank you,

CheckPoint | Effective Background Screening Services

888-534-1233 | Phone
888-332-4128 | Fax
info@checkpointscreening.com

Print Form