

**LPS INC.**  
**MEMBERSHIP APPLICATION- LANDLORDS**

**LPS INC. Service Application-Landlord/Owners/Property Management**

Every field on this Application MUST be completed. If not applicable, you must write N/A. Failure to fully complete this application in its entirety and return it along with the signed Certification (attached) will delay and/or deny your approval.

Principal Information (User Owner or Officer signing below)

Principal Name/Owner		Work Phone Number	
Home Address		Fax Number	
City/State/Zip			
Home Phone Number		Drivers License Number	
		Social Security Number	
Email address:		Cell Number:	
Authorized User's Name		Authorized User's E-mail Address (to set up account)	
Rental Property Address:		City	St ZIP

**FCRA Information**

For the Purposes of the FCRA, please check what you will be using this service for. (required).
Please indicate your intended use of information (check all that apply):
<input type="checkbox"/> Employment purpose (USER WILL IDENTIFY TO THE PROVIDER EACH TIME A REPORT IS REQUESTED FOR THIS PURPOSE). <input type="checkbox"/> Tenant screening. <input type="checkbox"/> Other. _____

Tenant Screening Attachment Information

<b>Are you an individual Landlord?</b>		
<input type="checkbox"/> Yes	<input type="checkbox"/> No	If yes, you must provide the following
<input type="checkbox"/> Copy of title <b>or</b>	<input type="checkbox"/> Copy of a utility bill <b>or</b>	<input type="checkbox"/> Copy of Drivers License
<input type="checkbox"/> Copy of property tax document	<input type="checkbox"/> Property insurance documents	

Bona Fide Business Verification

If you are a property management company/real estate office, a copy of your business and/or real estate license must be provided; along with <b>one</b> of the following:		
<input type="checkbox"/> Copy of Business License (must be attached if required by your state, city or county and if not required, two of the other items must be chosen and attached) Copy of property tax document	<input type="checkbox"/> Articles of Incorporation / Partnership	<input type="checkbox"/> Corporation verification with State or Federal government
<input type="checkbox"/> Sales tax records	<input type="checkbox"/> State and/or Federal tax records	<input type="checkbox"/> Professional State Issued License
<input type="checkbox"/> State Tax ID Certificate (not application)	<input type="checkbox"/> Federal ID No. form (not application)	<input type="checkbox"/> Proof of 501 (c) (3) status (non-profit, charitable, religious or educational organization)
	<input type="checkbox"/> Proof of status under FCRA § 621(b) (1, 2, 3) (Federal bank, CU, air/ground carries and those subject to the Packers and Stockyards Act of 1921)	

<b>Each of the following must be attached:</b>		
<input type="checkbox"/> Advertising Material or Business Card	<input type="checkbox"/> Copy of voided Business Check (only if sole proprietorship, partnership or corp. in business under 1 year)	<input type="checkbox"/> Copy of Principal's Photo ID / Drivers License
<input type="checkbox"/> Copy of Current Business Phone Bill		

# SERVICE AGREEMENT

This Service Agreement ("Agreement") is hereby entered into by and between LPS Data, Inc., dba Landlord Protection Service, Inc., a Washington Corporation ("Company" or "CRA") and the undersigned entity ("Client" or "End User").

## Client Certification of Permissible Use Under the Fair Credit Reporting Act (FCRA)

The Client certifies that all requests for information from LPS Data, Inc., and any reports received, will be made and used solely for purposes permitted under the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) and the Washington Fair Credit Reporting Act (RCW 19.182.020).

### Please select the applicable permissible purpose:

- Employment purposes** — with the written consent of the individual being screened (see 15 U.S.C. § 1681b(a)(3)(B)).
- Tenant screening purposes** — with the written consent of the individual being screened (see 15 U.S.C. § 1681b(a)(2)).

The Client agrees to promptly notify LPS Data, Inc. if it intends to request a report for any purpose other than the one selected above.

**Important Notice: Under the FCRA, any person who knowingly and willfully obtains consumer information under false pretenses may be subject to fines under Title 18 of the United States Code, imprisonment for up to two years, or both.**

For Tenant Screening purposes - The Client hereby represents and warrants that it is the landlord or the duly authorized agent of the landlord and is solely responsible for making all rental determinations with respect to each applicant screened. For Employment Screening purposes – The client hereby represents and warrants that it is the Employer or the duly authorized agent of the employer and is solely responsible for making all employment or hiring decisions with respect to each applicant screened. The Client further certifies that it is the ultimate end user of all consumer reports provided by the Company and agrees that such reports shall not be sold, assigned, distributed, or otherwise disclosed to any third party.

The Client certifies that all rental and/or employment decisions will be made in accordance with lawful policies and procedures and in full compliance with all applicable federal, state, and local laws and regulations. The Client further acknowledges and understands that the Company's employees are not authorized to provide legal advice or render legal opinions regarding the information contained in any consumer report.

## SERVICES

LPS data, Inc. may provide the following services, as requested by the Client: credit report or summary, criminal records, sex offender records, eviction/civil court records, motor vehicle records and driver's license information, worker compensation records, social security verifications, Identity verifications, education records, military records, employment verifications, rental verifications, references, and other background screening data related to the consumer's character, general reputation, personal characteristics and mode of living.

## WARRANTIES AND INDEMNIFICATION

LPS Data, Inc. compiles information from a variety of sources, including, without limitation, consumer reporting agency databases containing public record data, other information repositories, court record databases, and third-party researchers. The Client acknowledges that such sources are not owned, operated, or controlled by LPS Data, Inc. and, accordingly, LPS Data, Inc. does not guarantee or ensure the absolute accuracy, completeness, or timeliness of the information obtained therefrom. LPS Data, Inc. maintains procedures reasonably designed to promote the maximum possible accuracy of reported information and to respond in a timely manner to disputes or claims of inaccuracy in accordance with applicable law.

The Client further acknowledges that all information contained in the screening report provided by LPS Data, Inc. is obtained from third-party sources on an "AS IS" basis and is provided to the Client on an "AS IS" basis. TO THE MAXIMUM EXTENT PERMITTED BY LAW, LPS DATA, INC. DISCLAIMS ANY AND ALL REPRESENTATIONS AND WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE OR IMPLIED WARRANTIES ARISING FROM THE COURSE OF DEALING OR A COURSE OF PERFORMANCE; LPS DATA, INC. EXPRESSLY DISCLAIMS ANY AND ALL SUCH REPRESENTATIONS AND WARRANTIES.

The Client agrees to indemnify, defend, and hold harmless LPS Data, Inc. and its parents, affiliates, subsidiaries, successors, and assigns, and each of their respective officers, directors, employees, agents, vendors, and service providers, from any and all third-party claims, demands, actions, causes of action, liabilities, damages, losses, judgments, settlements, penalties, fines, costs, and expenses (including, without limitation, reasonable attorneys' fees and expenses) arising out of or relating to: (i) any breach of this Agreement or of any

representation, certification, or warranty made by the Client herein; (ii) the Client's violation of any applicable federal, state, or local law, rule, or regulation; and/or (iii) the Client's negligence, misconduct, recklessness, or errors or omissions.

The Client acknowledges that the Company is not a law firm and does not provide legal advice or legal opinions. Any documents, communications, or information provided by the Company in connection with the procurement or use of background screening reports are for informational purposes only and shall not be construed as legal advice. The Client agrees to consult with its own legal counsel regarding all legal matters related to the acquisition and use of consumer reports and investigative consumer reports, including, without limitation, compliance obligations and adverse action procedures.

The Client further acknowledges that any sample forms or documents made available by the Company—including, without limitation, disclosure forms, authorizations, criteria guidelines, and adverse action notices—are provided solely as a courtesy. Such materials do not constitute legal advice, and applicable laws governing their content are subject to change. The Client agrees to consult with legal counsel to ensure that any documents used comply with all applicable federal, state, and local laws and regulations.

Use of any such sample forms, documents, or processes, in whole or in part, is entirely at the Client's sole discretion and risk. To the extent the Client elects to use such materials, the Client agrees that they shall be deemed the Client's own documents and not those of the Company. The Client further agrees to indemnify, defend, and hold harmless the Company and its affiliates, vendors, and service providers, and their respective officers, directors, and employees, from and against any and all claims, liabilities, damages, losses, costs, and expenses (including reasonable attorneys' fees) arising out of or in connection with the Client's use of such materials.

## **REMEDIES**

LPS Data, Inc.'s liability for any alleged damages arising out of or relating to services provided to the Client shall be limited solely to the amount of actual, direct damages incurred by the Client. Notwithstanding the foregoing, in no event shall the Company's aggregate liability under this Agreement exceed an amount equal to three (3) times the average monthly fees paid by the Client to the Company for screening services during the calendar year in which the claim arose. **IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE SCREENING SERVICES, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.** The parties acknowledge and agree that the fees charged for the services provided hereunder reflect the allocation of risk set forth in this provision. This section constitutes the Client's sole and exclusive remedy against the Company for any and all claims arising out of or relating to this Agreement or the services provided hereunder.

## Compliance Assurances

User agrees, acknowledges and warrants, as a user / distributor of various credit related products and services, (the "Reports") that as applicable:

1. It shall and it shall cause its customers ("Customers") to abide by and accept responsibility for accessing, processing and using the Reports in accordance with the Fair Credit Reporting Act, 15 U.S.C. §1681 et. seq., ("FCRA") as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") and thereafter from time to time, the Gramm-Leach-Bliley Act of 1999 ("GLB Act"), the Driver Privacy Protection Act ("DPPA"), the laws of the applicable state issuing Motor Vehicle Records ("MVRs"), and with the requirements of the credit bureaus and database providers providing access to the Reports, as well as all other applicable local, state and federal laws governing access to the Reports; and
2. It shall and it shall cause its Customers to obtain a proper release and authorization from each job applicant and credit application from each credit applicant prior to requesting a Report on that applicant; and
3. Prior to requesting each consumer report, User shall and cause its Customer to identify the end user ("end user") of the consumer report, certify each permissible purpose for which the consumer report will be used and certify that the consumer report will be used for no other purpose, as defined by Section 607 of the FCRA; and
4. Compliance and keeping up to date with new requirements or laws is the responsibility of User and Customers; and
5. User understands and shall cause Customers to understand that a log must be maintained on consumer report information, with transaction details, for a minimum of sixty (60) months; and
6. User agrees and shall cause Customers to agree that it will secure consumer reports on individuals solely for its use in credit, collection, underwriting or employment transactions between itself and the individual to whom information refers and/or for such other "permissible purposes" related to a business transaction as are defined by the FCRA and that it will neither request nor use any such information for any other purpose; and
7. User further agrees and shall cause Customers to take all reasonable precautions to ensure that the Reports and consumer report information on individuals will be held in strict confidence, disclosed only to those of its employees whose duties reasonably relate to the legitimate business purpose for which the information was requested and not disclosed to any other person in whole or in part unless required by valid subpoena or court order; and
8. Consumer questions or comments regarding Reports shall be provided to the CRA providing same, with the CRA's name, address and telephone number provided to any consumer that is the subject of the disputed Report; and
9. It is understood that an independent third party "Site Inspection" of User and/or Customer's business location may be necessary prior to accessing consumer or other reports, for which a fee will be assessed. In accordance with the FCRA as well as credit bureau and data repository policies, as part of the investigation, credentialing and processing of this Application, User and its principal (owner or officer) signing below, understands, consents and authorizes that a criminal, consumer

credit and other background checks from a database Repository, Credit Bureau or Consumer Credit Reporting Agency, as applicable, may be obtained on User's business and its principal, to determine background, credit worthiness, credit standing and credit capacity, as applicable to User. The signature of User's authorized representative acknowledging acceptance of the above terms and conditions is set forth at the end of the attached Certification.

### Security Requirements

In signing the Agreement for use of services allowing access to and receipt of consumer or other non-public personally identifiable information, the undersigned User agrees to adhere to the following measures:

#### Data Access Security

We must work together to protect the privacy of consumers. The following measures are designed to reduce unauthorized access of consumer credit reports and other non-public personally identifiable information.

1. You must protect your account numbers and passwords so that only key personnel know this sensitive information. Unauthorized persons should never have knowledge of your passwords. Do not post or leave such information unattended in any manner.
2. System access software, whether developed by your company or purchased from a third party vendor, must have your account numbers and passwords "hidden" or embedded and be known only by supervisory personnel. Assign each user of your system access software a unique logon password.
3. Do not discuss your account numbers and passwords by telephone with any unknown caller, even if the caller claims to be an employee of a Credit Bureau or other data Repository.
4. Restrict the ability to obtain consumer credit and other information to only a few key personnel.
5. Point of sale customers utilizing the drivers license scanning product must make consumers aware via posters and obtain written consent that drivers license data is being collected and such will be used for fraud prevention and transaction dispute resolution and will not be used for marketing.
6. Place all terminal devices used to obtain consumer credit and other information in a secure location within your facility. You should secure these devices so that unauthorized persons cannot access them.
7. After normal business hours, be sure to turn off and lock all devices or systems used to obtain or store consumer credit and other information.
8. Secure hard copy and electronic files of consumer credit and other information within your facility to prevent unauthorized access.
9. Shred or destroy all hard copy consumer credit and other information when no longer needed in accordance with applicable contract, Repository regulation or law.
10. Erase or scramble electronic files containing consumer credit and other information when no longer needed in accordance with applicable contract, Repository regulation or law.
11. Advise all employees that your company can access consumer credit and other information only for the "permissible purposes" listed in your Agreement and that they may not, even for testing purposes, access their own consumer credit report or that of a family member, friend, public figure or celebrity, if your company does not have permissible purpose.

#### Record Retention

It is important that you keep consumer credit applications and reports for a reasonable period of time. This will help to facilitate the investigative process if a consumer claims that your company inappropriately accessed their credit and or other report. (Note: Your Agreement and some Repositories and/or Bureaus require 60 months, some require 36 months or even 72 months and The Federal Equal Credit Opportunity Act maintains that a creditor must preserve all written or recorded information connected with an application for 25 months.)

*"Under Section 621 (a) (2) (A) of the Fair Credit Reporting Act, 15 U.S.C. §1681 et. seq., ("FCRA"), as amended from time to time, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than \$2,500.00 per violation.*

Internal Systems Security

Internal Systems that have access to sensitive consumer or other non-public personally identifiable information, including those of your customers who will have access to your system, should implement the following security measures on their systems.

1. Use of screensavers (15 minute timeout maximum) for all personnel should be mandatory.
2. User Names and password rules must be set according to the **User Name and Password Security** section herein.

#### Application Security

When building an application system that will request, house or display sensitive consumer or other non-public personally identifiable information to an end user, the following measures must be put in place to help ensure unauthorized access of such data.

1. Technical measures to prevent screen scraping or robotic harvesting of any consumer or other non-public personally identifiable information, including information that can be viewed prior to purchasing a product, as well as contractual prohibitions on end users' right to screen scrape or robotic harvest.
2. The system should be set up so that account velocity is automatically measured and monitored for unusual activity. The system should also have the ability to turn off an individual account's access to consumer or other non-public personally identifiable information, if the account velocity threshold is tripped, and shut down access within 15 minutes if the site velocity threshold is tripped.
3. User Names and password rules must be set according to the **User Name and Password Security** section herein.

4. IP address restrictions are required for all users who will be accessing sensitive consumer or other non-public personally identifiable information. The IP address of the end user who is accessing the system must be known and set up to have such access in order to view sensitive consumer or other non-public personally identifiable information. The system must not allow users to access the system from an unknown or foreign IP address.
5. All transactions, XML and Web Based Applications must be sent over an encrypted medium. Valid encryption strategies are either HTTPS (SSL) V3 or better and at least 128 bit or HTTP over an IP Secure VPN.

User Name and Password Security

The following rules must be implemented when establishing User Names and passwords:

1. User Names must be at least Eight (8) characters in length.
2. All passwords must be at least fourteen (14) characters in length.
3. User Names and passwords cannot be the same.
4. Passwords cannot contain the User Name.
5. All passwords must contain any three (3) of the following: alphabetic characters, upper case, lower case, numeric characters, or symbol characters.
6. All Users must have a unique User Name and password.
7. Passwords should not be written down anywhere and User Names and passwords may not be shared.
8. Users must change their passwords at a minimum of once every 90 days.
9. Users' account and access shall be suspended after three (3) unsuccessful login attempts.
10. Security administrators should be notified immediately if the User has any reason to believe their User Name or password may have been compromised.
11. Inactive Users should be suspended after 90 days.
12. All suspended Users must change their passwords upon their next login.

Exception List

Notwithstanding the above, the credit bureaus and data repositories have identified certain types of companies to which consumer information cannot be sold. We have chosen to be even more restrictive and will not sell consumer information to:

- Credit or Financial Repair or Counseling (unless for non-profit, housing counseling or registered securities broker).
- Lawyers or Law Firms (unless sole practice is collections or those filing consumer bankruptcies or for employment).
- Private Investigator, Detectives or Law Enforcement (unless sole use is for employment purposes and an individual certification of permissible purpose is provided each time a report is requested).
- News Agencies or Journalists (unless sole use is for employment purposes or the review of a subscriber's credit and an individual certification of permissible purpose is provided each time a report is requested).
- Bail Bonds business or Repossession company (unless business is established, reputable or state licensed).
- Pawn Shop (unless business is reputable and in a secure and safe location).
- Process Server, Dance Studio, Check Cashing, Spiritual, Tattoo, Health, Book Club, Adult, Dating, Massage Service
- Companies: a) not in the traditional financial services industry; b) not routinely needing consumer reports in the ordinary course of business; c) providing reports direct to consumers; d) with questionable reputations or ethical natures or no legitimate need for consumer reports; e) officers or employees involved in credit fraud or other unethical business practices; or f) identified by a credit bureau or data repository as restricted.

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	Responsibility of Furnishers of Information to Consumer Reporting Agencies

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

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 initiated by the subject

of the report such as tenant screening, 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.

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 and state statutes and regulations in the locale you operate.

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

### [FACT Act Summary & Notices](#)

Following a public comment period, the Federal Trade Commission issued final summaries of identity theft and general consumer rights and revised furnisher and user notices under the FCRA and the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Consumer reporting agencies are required to notify consumers of their rights under FACTA and steps they can take to protect themselves against identity theft and difficulties resulting there from.

The identity theft rights summary includes the major new identity theft rights granted to consumers by FACTA, including the right to place fraud alerts on their credit reports, to block businesses and credit bureaus from reporting information in their credit files that is a result of identity theft, and to obtain from businesses information about accounts or transactions in their name that result from identity theft. The identity theft rights summary will be provided by consumer reporting companies to consumers who contact the agencies because they believe they are victims of fraud or identity theft.

The general consumer rights summary includes, among other things, consumers' right to see their credit files and know when they have been used against them, to correct inaccuracies, and to opt-out of unsolicited offers. The summary also notes that, in addition to identity theft victims, active duty military personnel have additional rights under the FCRA and FACTA. This general summary of rights updates the current summary, which credit reporting companies provide to consumers with their credit reports. The furnisher and user notices explain to businesses their duties under the FCRA.

The FTC received 50 comments from individuals, businesses, and associations. In response to these comments, the Commission has made some changes to the proposed summaries and notices it issued in July 2004, including: (1) the addition of a Spanish-language statement at the top of the summary of rights indicating where Spanish-speaking consumers may go to obtain more information in Spanish; (2) clarification that a consumer must contact the nationwide consumer reporting companies to request that a fraud alert be placed on his or her credit file, and that the initial alert remains in a consumer's file for at least 90 days; and (3) clarification that a consumer may request that a consumer reporting company block any information, not just account information, in the consumer's file if the information is the result of identity theft.

The FTC vote to approve the final rule and the publication of the Federal Register notice was 5-0.

To view the summary and notices, please click below or visit our website or contact us to request copies.

FCRA: <http://www.ftc.gov/os/statutes/031224fcra.pdf>

GLBA: <http://www.ftc.gov/privacy/glbact/glboutline.pdf>

DPPA: <http://www.nydmv.state.ny.us/forms/mv15dppa.pdf>

ADA: <http://www.sba.gov/ada/smbusgd.pdf>

Summaries of Rights and Notices of Duties Under the FCRA and FACT Act: Publication of Final Guidance on Model Disclosures:  
<http://www.ftc.gov/os/2004/11/041119facta.pdf>

Appendix E: Summary of Consumer Identity Theft Rights: Remediating the Effects of Identity Theft:  
<http://www.ftc.gov/os/2004/11/041119factaappe.pdf>

Appendix F: Summary of Consumer Rights Under the FCRA:  
<http://www.ftc.gov/os/2004/11/041119factaappf.pdf>

Appendix G: Notice to Furnishers of Information: Obligations of Furnishers Under the FCRA:  
<http://www.ftc.gov/os/2004/11/041119factaappg.pdf>

Appendix H: Notice to Users of Consumer Reports: Obligations of Users Under the FCRA:  
<http://www.ftc.gov/os/2004/11/041119factaapph.pdf>

## California Civil Code Section 1785.14(a) End User Compliance Certification

Section 1785.14(a), as amended, states that a consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will only be used for a permissible purpose unless all of the following requirements are met:

Section 1785.14(a)(1) states: "If a prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name."

Section 1785.14(a)(2) states: "If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the retail seller must certify, in writing, to the consumer credit reporting agency that it instructs its employees and agents to inspect a photo identification of the consumer at the time the application was submitted in person. This paragraph does not apply to an application for credit submitted by mail."

Section 1785.14(a)(3) states: "If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed."

In compliance with Section 1785.14(a) of the California Civil Code, by the signature of User's authorized representative acknowledging acceptance of the above terms and conditions set forth at the end of the attached Certification, User hereby certifies and shall cause end users to certify to the Consumer Reporting Agency as indicated above, whether it is or is not a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale").

User also certifies that if it or the end user is a Retail Seller who conducts Point of Sale transactions, it will, beginning on or before July 1, 1998, instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person.

User also certifies and shall cause end users to certify that it will only use the appropriate end user code number designated by the Consumer Reporting Agency for accessing consumer reports for California Point of Sale transactions conducted by Retail Seller.

If User and/or end user is not a Retail Seller who issues credit in Point of Sale transactions, it agrees that if it, at any time hereafter, becomes a Retail Seller who extends credit in Point of Sale transactions, it shall provide written notice of such to the Consumer Reporting Agency prior to using credit reports with Point of Sale transactions as a Retail Seller, and shall comply with the requirements of a Retail Seller conducting Point of Sale transactions, as provided in this certification.

## Certification

User has selected to utilize certain consumer products that are governed by the FCRA and Credit Bureau / Repository guidelines. Therefore, User must read all above sections and certify below that User is and will remain in compliance.

In whole or in part, LPS inc. reserves the right, in its sole discretion, at any time and for any reason, with or without prior written notice, via email, fax, or regular US mail and with no liability to User, to modify, amend, change, alter, update, add to or delete from the terms and conditions contained in this Application and User's agreement for access to consumer credit and other personally identifiable information per Credit Bureau / Repository, vendor, legal, industry, LPS INC or other mandate and audit User's compliance therewith as well as the legal requirements applicable thereto, via on-site visits, notifications and/or document requests, with the date of receipt deemed to be the effective date of the notice.

For questions please call: 1-800-577-8282. The signed Certification, along with the fully completed Application, must be sent in their entirety to: LPS INC, Attn: MEMBERSHIP ADMIN FAX 800-577-3799 or emailed to [Brandon@lpsdata.com](mailto:Brandon@lpsdata.com) or mailed to LPS Inc. 16625 Redmond Way PMB M446, Redmond WA. 98052

**By initialing next to each item to verify compliance, User certifies that:**

- \_\_\_\_\_ It has read, is and will remain in compliance with the **Notice to Users of Consumer Reports: Obligations of Users Under the FCRA**
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Summary of Your Rights Under the Fair Credit Reporting Act**
- \_\_\_\_\_ It has read and accurately and fully completed the **Application** section
  - Complete all appropriate sections. Be sure to include principal information.
  - Read each item listed in the FCRA section and initial choice of use and permissible purpose.
  - Select and attach the chosen items listed in the Bona Fide Business Verification Section. Also attach a copy of a voided business check/or personal check if individual landlord , a copy of photo id and advertising material or business card.
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Compliance Assurances** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Security Requirements** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Permissible Purpose Guidelines** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **FCRA Requirements** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Fact Act Summary & Notices** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **Summary of Consumers Rights** section
- \_\_\_\_\_ It has read, is and will remain in compliance with the **CA Civil Code End User Compliance** section
- \_\_\_\_\_ It is responsible for sending the “adverse action” letter to applicants who are denied or conditionally approved.

User certifies that the terms on this and the prior pages have been read, the information is accurate and that the undersigned agrees to all of the above terms and conditions as written on behalf of User and represents that he / she is authorized to execute on behalf of User and that facsimile signatures shall be construed as valid and binding marks.

By signing below, User confirms that they have a “permissible purpose” to access consumer reports and agree to comply with all terms and conditions outlined above, as well as the Service Agreement in its entirety. User further agrees to release LPS Data, Inc. and its subsidiaries from any claims, damages, or liabilities arising from the provision of consumer report information to me, my company, or any authorized agents. I acknowledge that LPS Data, Inc. may modify or terminate this agreement at any time.

User acknowledges that, under HUD Disparate Impact Guidelines, blanket policies regarding criminal convictions are not permitted. Criminal history must be evaluated on a case-by-case basis, taking into account the nature and severity of the offense and the time elapsed since the activity.

User understands that if they charge an applicant a screening fee, Washington State law requires each applicant to be provided a copy of the written rental criteria. Users must obtain a signed acknowledgement of this screening criteria before ordering a screening report.

User further understands that any applicant subject to an adverse action—including, but not limited to, denial of tenancy or the imposition of a higher deposit or cosigner—must be provided with a completed Adverse Action form.

For properties located within the City of Seattle, User acknowledges that under Seattle’s Fair Chance Ordinance (SMC 14.09), landlords are prohibited from requiring disclosure of, inquiring about, rejecting an applicant based on, or taking adverse action due to arrest records, conviction records, or criminal history, except for registry information as specified in subsections 14.09.025.A.3, 14.09.025.A.4, and 14.09.025.A.5, and subject to the exclusions and requirements set forth in Section 14.09.115.

\_\_\_\_\_  
Landlord Name

\_\_\_\_\_  
Signature of Owner

\_\_\_\_\_  
Name Typed or Printed

\_\_\_\_\_  
Date



# Protection Service, Inc.

## Payment Agreement

I agree to pay all services requested, in full at time of request. I also understand that if the amount billed should be declined by my credit card provider, the service I have requested will not be processed.

\_\_\_\_\_ Signed \_\_\_\_\_  
Date

Card Type: (check one)

MasterCard \_\_\_\_\_

Visa \_\_\_\_\_

American Express \_\_\_\_\_

Quantity	Description	Price	Amount
	LPS application Fee:	\$75.00	
	Payable to- LPS INC.		
		Tax	Included
	<b>SALE SLIP</b>	<b>Total</b>	\$75. 00

Card number: \_\_\_\_\_ Exp Date: \_\_\_\_\_

Security code \_\_\_\_\_

Name on Card: \_\_\_\_\_

Address Used for Credit Card: Street \_\_\_\_\_

City \_\_\_\_\_ St \_\_\_\_\_ Zip \_\_\_\_\_

Purchaser Sign Here: X \_\_\_\_\_

Cardholder acknowledges receipt of goods or services in the  
Amount of the Total shown here on and agrees to perform the Obligations set forth in the Cardholders agreement.

**Merchant copy**



LPS INC. Getting Started Check List:

1.) COMPLETE AND SIGN APPLICATION FOR MEMBERSHIP

2.) COMPLETE, INITIALING WHERE NEEDED, AND SIGN SERVICE AGREEMENT, AND CREDIT CARD PAYMENT FORM.

3.) INCLUDE A COPY OF YOUR DRIVERS LICENSE & ALL REQUIRED ATTACHMENTS MENTIONED ABOVE

**\*\* \$75.00 SET UP FEE WILL BE CHARGED TO YOUR CREDIT CARD. This is a onetime set up fee.**

**All Clients:**

- Must use the LPS Inc. Rental Applications or online application system
- Must require proof of ID from the applicant, provide a copy of the screening criteria to the applicant, and obtain a signed acknowledgement of screening criteria prior to placing the order for a background check.
- If you deny the application or ask for added security or a co-signer you will need to send out an "Adverse Action" letter to the applicant.
- All forms that you need should be found on our website to stay in compliance with the Fair Credit Reporting Act and the Washington State Fair Tenant Screening Act.

**This membership can be faxed 800-577-3799 or scanned and emailed to [brandon@lpsdata.com](mailto:brandon@lpsdata.com).**