

Liberty Alliance Inc. Service Agreement

This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument. A signature on a copy of this Agreement received by either party by facsimile is binding upon the other party as an original. The parties shall treat a photocopy of such facsimile as a duplicate original. The individual accepting and executing this document represent that he or she is authorized to do so.

Liberty Alliance, Inc. strives to deliver accurate and timely information products to assist your company (hereinafter "End-User") in making intelligent decisions for a permissible purpose under applicable law. To this end, Liberty Alliance, Inc. assembles information from a variety of sources, including databases maintained by consumer reporting agencies containing information from public records, other information repositories and third-party researchers. Please understand that these information sources and resources are not maintained by Liberty Alliance, Inc. Therefore, it cannot be a guarantor that the information provided from these sources is absolutely accurate or current. Nevertheless, Liberty Alliance, Inc. has in place procedures designed to respond promptly to claims of incorrect or inaccurate information in accordance with applicable law.

End-User's Certification of FCRA Permissible Purpose(s)

End-User certifies that all of its orders for information products from Liberty Alliance, Inc. shall be made, and the resulting reports shall be used, for the following Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., permissible purposes only:

Reseller hereby certifies that it will request the Services and the information therein from Experian and resell such to its customers solely for said customers' use in connection with (a) credit granting; (b) collections; (c) employment; (d) insurance underwriting; (e) child support enforcement when in full compliance with the provisions of the FCRA; or (f) governmental licensing transactions between the customer and the Consumer about whom the credit information relates, and will not request, use or resell any such Services or information for any other purpose, regardless of whether permitted by law.

FCRA Requirements

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 the End-User 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.

Liberty Alliance, Inc. strongly endorse the letter and spirit of the Federal Fair Credit Reporting Act. Liberty Alliance, Inc. believes 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, Liberty Alliance, Inc. expects that the End-User and its staff will comply with all relevant federal statutes and the statutes and regulations of the states in which the End-User operates.

End-User's Certification of Legal Compliance

End-User certifies to Liberty Alliance, Inc. that the information products it receives will not be used in violation of any applicable federal or state laws. End-User accepts full responsibility for using the information products it receives from Liberty Alliance, Inc. in a legally acceptable fashion and the consequences of use and/or dissemination of those products. End-User further agrees to put into place reasonable procedures for the fair and equitable use of background information and to secure the confidentiality of private information. End-User agrees to take precautionary measures to protect the security and dissemination of this information including, for

example, restricting terminal access, utilizing passwords to restrict access to terminal devices, and securing access to, dissemination and destruction of hard copy reports. End-User agrees to abide by the security requirements listed in the Access Security Requirements attached to this Agreement as Addendum A, and Inc. fully herein. Likewise, as a condition of your entering into this Agreement, you will be required to certify that End-User also has in place reasonable procedures designed to comply with all applicable state and federal laws. You also will be required to certify that End-User will retain any information it receives from Liberty Alliance; Inc. for a period of five years from the date the report was received.

A. When Information Products are used for Employment Purposes

If the information products End-User obtains from Liberty Alliance, Inc. are to be used for an employment purpose, End-User certifies that prior to obtaining or causing a “consumer report” and/or “investigative consumer report” to be obtained, a clear and conspicuous disclosure, in a document consisting solely of the disclosure, will be made in writing to the consumer explaining that a consumer report and/or investigative consumer report may be obtained for employment purposes. This disclosure will satisfy all requirements identified in Section 606(a)(1) of the FCRA as well as any applicable state or local laws. The consumer will have authorized, in writing, the obtaining of the report by End-User.

If the consumer is denied employment, or other adverse employment action taken based in whole or in part on the information products provided by Liberty Alliance, Inc., End-User will provide to the consumer: (1) a copy of the report; and (2) a description, in writing, of the rights of the consumer entitled: “A Summary of Your Rights Under the Fair Credit Reporting Act” and (3) the pre-adverse and adverse notifications as contemplated in the FCRA. End-User hereby acknowledges that it has received a copy of the Summary of Rights (16 C.F.R. Part 601, Appendix A) and Notice of User Responsibility (16 C.F.R. Part 601, Appendix C).

B. Disputing Consumer Reports

If the consumer makes a written request within a reasonable amount of time, End-User will provide: (1) information about whether an investigative consumer report has been requested; (2) if an investigative consumer report has been requested, written disclosure of the nature and scope of the investigation requested; and (3) Liberty Alliance’s contact information, including complete address and toll-free telephone number as indicated at the end of this Agreement. This information will be provided no later than five days after the request for such disclosure was received from the consumer or such report was first requested, whichever is the latter.

Additional Requirements for Moving Violation Reports (MVRs) and Driving Records

End-User hereby certifies that Moving Violation Reports and/or Driving Records (MVRs) shall only be ordered in strict compliance with the Driver Privacy Protection Act (“DPPA”, at 18 U.S.C. § 2721 et seq.) and any related state laws. End-User further certifies that no MVRs shall be ordered without first obtaining the written consent of the consumer to obtain “driving records,” evidence of which may be requested by, and transmitted to Liberty Alliance, Inc. in the form of the consumer’s signed release authorization form. End-User also certifies that it will use this information only in the normal course of business to obtain lawful information relating to the holder of a commercial driver’s license or to verify information provided by an applicant or employee. End-User shall not transmit any data contained in the resulting MVR via the public internet, electronic mail, or other unsecured means.

General Provisions

End-User agrees not to resell, sub-license, deliver, display or otherwise distribute to any third party any of the information products addressed herein, except as required by law or when authorized by the consumer in writing. End-User may not assign or transfer this Agreement without the prior written consent of Liberty Alliance, Inc. If any of the provisions of this Agreement become invalid, illegal or unenforceable in any respect, the validity, legality and enforceability of the remaining provisions shall not in any way be impacted. By agreement of the parties, California law shall guide the interpretation of this Agreement, if such interpretation is required. All litigation arising out of this Agreement shall be commenced in California, and the parties hereby consent to such jurisdiction and venue. Any written notice by either party shall be delivered personally by messenger, private

mail courier service, or sent by registered or certified mail, return receipt requested, postage prepaid to the addresses listed below. This Agreement shall be construed as if it were jointly prepared. Both parties agree that this Agreement constitutes all conditions of service, present and future. Changes to these conditions may be made only by mutual written consent of an authorized representative of End-User and an officer of Liberty Alliance, Inc. The headings of each section shall have no effect upon the construction or interpretation of any part of this Agreement.

If End-User is permitted to request consumer reports for employment purposes via Liberty Alliance, Inc.' website then, in addition to all other obligations, End-User agrees to abide by such additional conditions that may be imposed to utilize the website, provide all required certifications electronically, to maintain complete and accurate files containing all required consent, authorization and disclosure forms with regard to each consumer for whom a report has been requested, and maintain strict security procedures and controls to assure that its personnel are not able to use End-User's Internet access to obtain reports for improper, illegal, or unauthorized purposes. End-User agrees to allow Liberty Alliance, Inc. to audit its records at any time, upon reasonable notice given. Violations discovered by Liberty Alliance, Inc. might result in immediate termination of the account, legal action, and/or referral to federal or state regulatory agencies.

Fees and Payment

End-User agrees to pay nonrefundable fees and other charges for Liberty Alliance, Inc.' background check services. Full payment must be made within thirty (30) days of the invoice date. At Liberty Alliance, Inc.' option, payments not received thirty (30) days after the date of the invoice will cause the account to be placed on temporary interruption, with no additional requests being processed until the balance due is paid in full or arrangements have been made with Liberty Alliance, Inc.' Accounts Payable Department. Accounts with invoices unpaid (90) days or more will be assessed an interest charge of 5 ½ % per month, as allowed by applicable law. If the account goes to collection, End-User agrees to pay all collection expenses, including attorneys' fees and court costs. End-User agrees that providing credit card information and submitting it electronically to Liberty Alliance, Inc. represents a legal authorization to debit the card for the orders placed or for non-payment per the 30-day terms. End-User agrees that prices for services are subject to change without notice, although Liberty Alliance, Inc. will make every reasonable effort to give notice of such change before it becomes effective. Any account that remains inactive for a period of twelve (12) months will be deemed inactive and may be terminated by Liberty Alliance, Inc.

Warranties and Remedies

End-User understands that Liberty Alliance, Inc. obtains the information reported in its information products from various third party sources "AS IS", and therefore is providing the information to End-User "AS IS". Liberty Alliance, Inc. makes no representation or warranty whatsoever, express or implied, including but not limited to, implied warranties of merchantability or fitness for particular purpose, or implied warranties arising from the course of dealing or a course of performance with respect to the accuracy, validity, or completeness of any information products and/or consumer reports, that the information products will meet End-User's needs, or will be provided on an uninterrupted basis; Liberty Alliance, Inc. expressly disclaims any and all such representations and warranties. Liberty Alliance, Inc. will not be liable for any indirect, incidental, consequential, or special damages for loss of profits, whether incurred as a result of negligence or otherwise, even if Liberty Alliance, Inc. has been advised of the possibility of such damages. End-User agrees to indemnify and hold harmless Liberty Alliance, Inc., its successors and assigns, officers, directors, employees, agents and suppliers from any and all claims, actions or liabilities arising from or with respect to information products provided by it. Liberty Alliance, Inc. nevertheless agrees to be responsible for actual damages to the extent of and maximum stated herein for third party claims directly resulting from Liberty Alliance, Inc.' sole negligence in assembling the consumer report. Liberty Alliance, Inc.' maximum aggregate liability for damages in this regard shall not exceed an amount equal to the price paid by End-User to Liberty Alliance, Inc. for the consumer report(s) at issue. Liberty Alliance, Inc. does not guarantee End-User's compliance with all applicable laws in its use of reported information, and makes no effort to provide compliance related services in connection with its furnishing of reports. End-User understands that any conversation or communication with Liberty Alliance representatives regarding searches, verifications or other services offered by Liberty Alliance, Inc. are not to be considered a legal opinion regarding its use. End-User agrees that it will consult with its own legal or other counsel regarding the legality of using or relying on reported information in making employment decisions.

Term and Termination

The term of this Agreement shall begin on the date it is executed by End-User and will continue for a period of one (1) year from that date, unless earlier terminated in writing. This Agreement will renew automatically for successive one (1) year periods unless either party gives written notice to the other party of its intent to terminate the Agreement. Such notice of intent to terminate must be given no less than thirty (30) days prior to the proposed termination date. Liberty Alliance, Inc. may terminate or revise the provisions of this Agreement immediately upon written notice if End-User is the debtor in a bankruptcy action or in an assignment for the benefit of creditors or if End-User undergoes a change in ownership. Termination of this Agreement by either party does not release End-User from its obligation to pay for services rendered.

Force Majeure

User agrees that Liberty Alliance, Inc. is not responsible for any events or circumstances beyond its control (e.g., including but not limited to war, riots, and/or Acts of God) that prevent Liberty Alliance, Inc. from meeting its obligations under this Agreement.

I have read the above information starting with page 1 and ending with page 4, and agree to comply with all state and federal laws, the FCRA and Liberty Alliance, Inc. rules and policies.

Signature/Title

Date

Access Security Requirements

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

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

1. Implement Strong Access Control Measures

1.1 Do not provide your credit reporting agency Subscriber Codes or passwords to anyone. No one from the credit reporting agency will ever contact you and request your Subscriber Code number or password.

1.2 Proprietary or third party system access software must have credit reporting agency Subscriber Codes and password(s) hidden or embedded. Only supervisory personnel should know account numbers and passwords.

1.3 You must request your Subscriber Code password be changed immediately when:

- any system access software is replaced by another system access software or is no longer used;
- the hardware on which the software resides is upgraded, changed or disposed of.

1.4 Protect credit reporting agency Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).

1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.

1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.

1.7 Keep user passwords Confidential.

1.8 Develop strong passwords that are:

- Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- Contain a minimum of seven (7) alpha/numeric characters for standard user accounts

1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.

1.10 Active logins to credit information systems must be configured with a 30 minute inactive session, timeout.

1.11 Restrict the number of key personnel who have access to credit information.

1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of your membership application.

1.13 Ensure that you and your employees do not access your own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.

1.14 Implement a process to terminate access rights immediately for users who access credit reporting agency credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.

1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.

1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

2. Maintain a Vulnerability Management Program

2.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

2.3 Implement and follow current best security practices for Computer Virus detection scanning services and procedures:

- Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
- If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.
- On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.

2.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:

- Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.
- If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated.
- Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
- Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.

3. Protect Data

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)

3.2 All credit reporting agency data is classified as Confidential and must be secured to this requirement at a minimum.

3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all credit reporting agency data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.

3.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

4. Maintain an Information Security Policy

4.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.

4.2 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.

4.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.

4.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

5. Build and Maintain a Secure Network

5.1 Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.

5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

5.3 Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.

5.4 Any stand alone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

5.5 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.

5.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).

6.2 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access credit reporting agency systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:

- protecting against intrusions;
- securing the computer systems and network devices;
- and protecting against intrusions of operating systems or software.

Record Retention: *The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, the credit reporting agency requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.*

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

I have read the Access Security Requirements Addendum A, and agree to comply with these standards in conjunction with all state and federal laws, the FCRA and Liberty Alliance, Inc. rules and policies.

Signature/Title

Date

For all companies located in California, or doing business in California the following additional document must be completed. Please enter company name, circle appropriate End-User status, and sign.

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,

_____ ("End User") hereby certifies to
Consumer Reporting Agency as follows: Liberty Alliance, Inc. that

(Please circle) End User **(IS)** **(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").

End User also certifies that if End User is a Retail Seller who conducts Point of Sale transactions, End User 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.

End User also certifies that it will only use the appropriate End User code number designated by Consumer Reporting Agency for accessing consumer reports for California Point of Sale transactions conducted by Retail Seller.

If End User is not a Retail Seller who issues credit in Point of Sale transactions, End User agrees that if it, at any time hereafter, becomes a Retail Seller who extends credit in Point of Sale transactions, End User shall provide written notice of such to 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.

End User _____ Date: _____

Signature: _____ Title: _____