PHILLIPS AGENCY, INC.

Phillips Agency, Inc. User Agreement

This Agreement is made and entered into by and between Phillips Agency, Inc., ("Phillips Agency, Inc.") and the undersigned ("User"). This Agreement shall be effective at such time as Phillips Agency, Inc. has sent written notification, whether via facsimile, e-mail, or otherwise, to User indicating its acceptance of the terms and conditions of the Agreement (the "Effective Date").

Phillips Agency, Inc.'s Services: Phillips Agency, Inc. shall provide consumer reports and investigative consumer reports ("Screening Reports") at User's request in connection with any pre-employment or post-employment background screening of applicants (the "Applicant") or retention of employees (the "Employee"). Searches may include such information as employment history, consumer credit reports, motor vehicle records, education verifications, criminal and civil records, drug testing and other background information. In the case of investigative consumer reports, Phillips Agency, Inc. shall also provide personal references collected and processed by Phillips Agency, Inc. as requested by User through various channels of information.

Phillips Agency, Inc. as Agent of User: User acknowledges and agrees that Phillips Agency, Inc. is an authorized agent of User for the purpose of investigating, researching, preparing and returning the Searches ordered by User.

Information Security: User acknowledges and understands its obligation to maintain the confidentiality and integrity of any information and User identification numbers and passwords requested from or through Phillips Agency, Inc.

Compliance with Applicable Laws: User and Phillips Agency, Inc. shall comply in good faith with all applicable laws in the request, preparation, transmission, dissemination and use of Search Results, including, but not limited to, the FCRA, Title VII of the Civil Rights Act of 1964, the Equal Employment Opportunity Commission ("EEOC") guidelines and regulations, Consumer Reporting Act (California Civil Code Sections 1785.1 et seq.), Investigative Consumer California Civil Code Section 1786, et. seq.) and all other applicable laws and regulations relating to the use of consumer credit reports and consumer investigative reports.

Permissible Purpose: Subscriber certifies that consumer report information, as defined by the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq. ("FCRA"), will be ordered only when subscriber intends to use the credit information or consumer reports; (a) in accordance with the FCRA and all State law Counterparts, and (b) for one of the following permissible purposes: (i) in connection with a credit transaction involving the consumer on whom the consumer report is to be furnished and involving the extension of credit to or, review or collection of an account of, the consumer; (ii) in connection with the underwriting of insurance involving the consumer; (iii) as a potential investor for services, or current insurer, in connection with a valuation of, or an assessment for the credit or prepayment risks associated with an existing credit obligation; (iv) when subscriber otherwise has a legitimate business need for the account to determine whether the consumer continues to meet the terms of the accounts; (v) in accordance with the written instructions of the consumer to whom it relates; or (vi) for employment purposes. Subscriber will use each consumer report ordered from under the agreement for one of the foregoing purposes and for no other purpose.

_____(a) in connection with a credit transaction involving the consumer on whom the information is to be furnished and involving the extension of the credit to, or review or collection of an account of the consumer, or
_____(b) for employment purposes, or
_____(c) in connection with the underwriting of insurance involving the consumer
(to be initialed by the person signing on behalf of Subscriber)

User is a _____ and has a need for consumer credit information in connection with the evaluation of individuals for employment, promotion, reassignment or retention as an employee ("Consumer Report for Employment Purposes"0)

User's Obligations

Disclosure to Applicant or Employee. User shall provide Applicant or Employee with a clear and conspicuous disclosure, in writing, that the Background Report will be obtained for employment purposes and such disclosure shall be contained in a document containing only such disclosure. User shall provide Applicant or Employee such other disclosures as required by the FCRA and other applicable state and local laws for the type of report requested Background Report, and before taking any adverse action based in whole or in part upon any information contained in the report.

Written Authorization from Applicant or Employee: User shall obtain from the Applicant or Employee a written authorization to obtain and use the Background Report as required by the FCRA and all other applicable State and local laws.

Certification to Phillips Agency, Inc.: Concurrent with making the request for a Report, User shall provide Phillips Agency, Inc. with certification that complies with section 604(b)(1) of FCRA (15 U.S.C. §1681b(b)(1), and in the case of a Report that constitutes an investigative consumer report as defined by the FCRA, an additional certification in a form that complies with section 606(a)(2) of FCRA (15 U.S.C. §1681d(a)(2) and all other certifications as may be required by applicable state and local laws.

Use for Employment Purposes Only: User shall use the Background Report provided by Phillips Agency, Inc. for employment purposes only and shall not use the Background Report in violation of any Federal or State equal employment opportunity law or regulation. User shall notify Phillips Agency, Inc. immediately of any change in purpose for which the information is used.

User shall request Consumer Report for Employment Purposes pursuant to procedures prescribed by Reseller from time to time only when it is considering the individual inquired upon for employment, promotion, reassignment or retention as an employee, and for no other purpose. User shall comply with any federal and state laws which may restrict or ban the use of Consumer Repot for Employment Purposes.

Use for Permissible Purposes: User shall be the exclusive user of the Background Reports and certifies that such Screening Reports shall be used (a) solely for the permitted purposes as proscribed by Section 604 of the FCRA [15 U.S.C.§1681b], California Civil Code Section 1786.12 and all other applicable State and local laws; (b) solely for User's exclusive one-time use. User shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with User's own data, or otherwise in any service which is derived from the consumer reports. The consumer reports shall be requested by, and disclosed by User only to User's designated and authorized employees having a need to know and only to the extent necessary to enable User to use the Consumer Reports in accordance with this Agreement. User shall ensure that such designated and authorized employee shall not attempt to obtain any Consumer Reports on themselves, associates, or any other person except in the exercise of their official duties.

Use of TransUnion Scores: User will request Scores only for User's exclusive use. User may store scores solely for User's own uses in furtherance of User's original purpose for obtain the Scores. User shall not use the Scores for model development or model calibration and shall not reverse engineer the Score. All Scores provided here under will be held in strict confidence and may never be sold, license, copied, reused, disclosed, reproduced, revealed or made accessible in whole or part, to any person, except (i) to those employee of User with a need to know and in the course of their employment; (ii) to those third party processing agents and other contractors of User who have executed an agreement that limits the use of the Scores by the third party only to the use permitted to User and contains the prohibition set forth herein regarding model development, model calibration, reverse engineering and confidentiality; (iii) when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score;(iv) to government regulatory agencies; or (v) as required by law.

Basis for Employment Decisions and Obligations after Adverse Decisions: User shall base all employment decisions and actions on its own policies and procedures and acknowledges and agrees that Phillips Agency, Inc.'s employees are not allowed and will not render any opinions regarding the Background Report. Before taking any adverse action against an Applicant or Employee based in whole or in part on any information provided in the Background Report provided by Phillips Agency, Inc. per FCRA guidelines, User and/or Phillips Agency, Inc. is required to provide the Applicant or Employee with a copy of their Background Report. User shall inform the Applicant or Employee that Phillips Agency, Inc. did not make the decision to take adverse action and cannot give specific reasons for the adverse action taken. User shall further provide a Summary of Rights under the FCRA to the Applicant or Employee.

Confidentiality and Security of Information. User acknowledges and understands its obligation to maintain the confidentiality and integrity of any information received by User. All information requested by User is for User's exclusive use and User shall take reasonable steps to ensure that all information provided by Phillips Agency, Inc. will be held in strict confidence, will be kept confidential and will not be disclosed to any third party not involved in the employment decision for which the information is sought. Any use of the Background Report provided by Phillips Agency, Inc., other than for the internal uses provided for in this contract is prohibited, including, but not limited to resale or other commercial use, misrepresentation, improper use of the information or access to the information by unauthorized personnel, whether intentionally or due to carelessness, and may subject User to criminal and/or civil liability under the Federal Credit Reporting Act ("FCRA") and other applicable Federal, State and local laws.

Protection of Access Codes: If User is issued an access code to be used for Internet access to Phillips Agency, Inc.'s services, the Code User shall only publicize the Access Code to personnel on a need-to-know basis. Any log-on or password information provided to User in connection with the Access Code shall be provided only to an "Account Administrator" and specific individuals designated as "Authorized Users". User shall notify Phillips Agency, Inc. immediately upon any change of the Account Administrator or Authorized Users.

Protection of Reports: User shall securely store any hard copy of a Background Report and protect it against release and disclosure to unauthorized personnel or third parties.

Payment Requirements/Collection: User Agrees to promptly pay for all services rendered hereunder in accordance with Phillips Agency, Inc.'s schedule of fees. Pricing is subject to change at any time with written notice. Notices will be sent to user 30 days prior to fee change. User agrees to pay all applicable charges within thirty (30) days of receipt of invoice. All monetary obligations to Phillips Agency, Inc. for services rendered which are past due thirty days or more may, at the discretion of Phillips Agency, Inc., bear interest at the rate of one and one-half percent (1½ %) per month and/or relinquish User's access privileges and release Phillips Agency, Inc. from any obligation to perform any further services. In the event that legal action is necessary to obtain the payment of any monetary obligations to Phillips Agency, Inc., the User shall be liable to Phillips Agency, Inc. for all costs and reasonable attorneys' fees incurred by Phillips Agency, Inc. in collection of such obligations.

Attorneys Fees and Costs: In the event a dispute arises with respect to this Agreement, the party prevailing in such dispute shall be entitled to recover all expenses, including, without limitation, reasonable attorneys' fees and expenses incurred in ascertaining such party's rights, and in preparing to enforce, or in enforcing such party's rights under this Agreement, whether or not it was necessary for such party to institute suit or submit the dispute to arbitration.

Arbitration of Disputes: Any controversy or claim arising out of or relating to this Agreement or the breach thereof, shall be settled by binding arbitration administered by mutually agreed upon arbitration service in accordance with its rules, and judgment upon the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof. The arbitration hearing and all proceedings in connection therewith shall take place in Toccoa, Georgia. The arbitration shall be conducted by one or more arbitrators selected by the parties from a panel of arbitrators. The arbitration hearing shall be commended within 90 days of the filing of a Demand for Arbitration by either party, and the award shall be rendered within 30 days of the conclusion of such hearing.

Governing Law: This Agreement is deemed to be made, executed and performed in the State of Georgia. This Agreement shall be governed by and shall be construed in accordance with the laws of the State of Georgia, without reference to principles of conflicts of laws. The parties to this Agreement consent to jurisdiction and venue in the State and Federal courts located in the State of Georgia, County of Stephens.

Waiver: The failure of either party to insist in any one or more cases upon the strict performance of any term, covenant or condition of this Agreement will not be construed as a waiver of a subsequent breach of the same or any other covenant, term or condition; nor shall any delay or omission by either party to seek a remedy for any breach of this Agreement be deemed a waiver by either party of its remedies or rights with respect to such a breach.

Successors: This Agreement shall inure to the benefit of and bind the heirs, personal representatives, successors, and assigns of the parties.

Limitation of Liability: Phillips Agency, Inc. and User agree that unless Phillips Agency, Inc. has committed gross negligence or
engaged in intentional wrongdoing in the preparation and transmission of the Background Report, Phillips Agency, Inc.'s total liability to User shall be limited to the return of the fees paid to Phillips Agency, Inc. for the Background Report and then only to the extent that the information contained in the Background Report

is found to be the primary basis upon which User incurred injury or damage resulting from the furnishing of the Background Report by Phillips Agency, Inc. Phillips Agency, Inc. and User agree that Phillips Agency, Inc. shall not be liable to User for any other damages, costs or expenses whatsoever except as expressly agreed to above or pursuant to Section 12 (a) hereof, and that neither party shall be liable to the other party for punitive, exemplary or consequential damages.

Warranty: Phillips Agency, Inc. represents and warrants that services will be performed in a diligent and professional manner in accordance with applicable industry standards. Phillips Agency, Inc. shall use its best efforts to provide high quality, timely and accurate information to User, however User recognizes that Phillips Agency, Inc. cannot guarantee the accuracy of the information provided because such information is obtained from public records and other third party sources that may not always be accurate or current. The Background Report obtained by Phillips Agency, Inc. is derived from databases and records that have been created and maintained by various government agencies, private companies, and other contributors that are not under the control of Phillips Agency, Inc. Responsibility for the accuracy of the information contained in the Background Report and these databases and records rests solely in the contributor. The User waives any and all claim or claims against Phillips Agency, Inc. arising out of or related to the accuracy of the Background Report, databases and records.

Term: The term of this Agreement shall continue in force and effect without any fixed date of termination; provided, however, that: either party may terminate this Agreement for any reason or no reason at all upon thirty (30) days prior written notice of termination subject to any and all obligations, responsibilities and liabilities incurred prior to termination; or User may terminate this Agreement, without prior notice, if the other party breaches any provision of this Agreement and fails to cure such breach within ten (10) calendar days after receiving written notice thereof; or Phillips Agency, Inc. may, with just cause, such as delinquency or violation of the terms of this Agreement or a legal requirement of this Agreement or any applicable Federal, State or local law, discontinue serving User and terminate this Agreement immediately.

_____
Company Name

_____ _____
Type or Print Name of Owner or Officer Title

X_____ _____
Authorized Signature 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 passwords to anyone. No one from the credit reporting agency will ever contact you and request your password.

1.2. Account numbers and passwords should be known only by supervisory personnel.

1.3 You must request your 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 password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your 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 six (6) 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 Restrict the number of key personnel who have access to credit information.

1.11 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.

1.12 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.

1.13 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.

1.14 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 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.

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 a period of 5 years from the date of the inquiry. In keeping with the ECOA, the credit reporting agency requires that you retain the credit application, release and authorization form and, if applicable, a purchase agreement for a period of not less than 5 years from the date of the inquiry. 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 or release 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.”

_____ _____

Authorized Signature Title Date

Glossary

Terms and Definitions

Computer Virus: A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.

Confidential: Very sensitive information. Disclosure could adversely impact our company.

Encryption: the process of obscuring information to make it unreadable without special knowledge.

Firewall: In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.

Information Lifecycle :(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.

IP Address: A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.

Peer-to-Peer: A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.

Router: A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.

Spyware: Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.

SSID: Part of the WI-Fi Wireless LAN, a service set identifier (SSID) is a code that identifies each packet as part of that network. Wireless devices that communicate with each other share the same SSID.

WEP Encryption: (Wired Equivalent Privacy) A part of the wireless networking standard intended to provide secure communication. The longer the key used, the stronger the encryption will be.

WPA: (Wi-Fi Protected Access) A part of the wireless networking standard that provides stronger authentication and more secure communications. Replaces WEP. Uses dynamic key encryption verses static as in WEP (key is constantly changing and thus more difficult to break than WEP).

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. Responsibilities of Furnishers of Information to Consumer Reporting Agencies
§ 628. Disposal of Records

Each of these sections is of direct consequence to users who 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 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. 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 statutes and the statutes and regulations of the states in which you operate.

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

_____ _____

Signature Title Date

PHILLIPS AGENCY, INC.

PHILLIPS AGENCY, INC.
CLIENT/USER CERTIFICATION
PURSUANT TO 15 U.S.C. 1681 B(B)

Pursuant to the Fair Credit Reporting Act 15 U.S.C. 1681-1681U, as amended by the Consumer Credit Reporting Reform Act of 1996 (the "Act"), _____, ("Client") hereby agrees, certifies and warrants to Phillips Agency, Inc. ("PHILLIPS AGENCY") as follows:

1. Client will not request, cause to be prepared or procure from PHILLIPS AGENCY, any consumer report for employment purposes unless:

a. Prior to requesting, causing to be prepared or procuring a consumer and / or investigative consumer report, Client provides the consumer a clear and conspicuous written disclosure informing him/her that a consumer and /or an investigative consumer report may be obtained for employment purposes, in a document consisting solely of the disclosure; and
b. Prior to requesting a consumer and /or investigative consumer report, Client obtains a written consent from the consumer specifically authorizing the procurement of a consumer and/ or investigative consumer report by that Client.

2. In using a consumer and/or investigative consumer report for employment purposes, before Client take any adverse action, based in whole or in part on the report, Client shall provide to the consumer to whom the report relates:

a. A copy of the consumer and /or investigative consumer report; and
b. A description in writing of the rights of the consumer under the Act, in the form attached here to as Attachment A, title "Consumer Summary."

3. In the event Client takes adverse action against a consumer, based in whole or in part on a consumer and/or investigative report prepared by Phillips Agency, Client shall provide the consumer Phillips Agency's name, address and telephone number.

4. In the event Client takes adverse action against the consumer, based in whole or in part on a consumer and/or investigative consumer report, Client shall provide the consumer with a statement that "PHILLIPS AGENCY did not make the decision to take adverse action and is unable to provide the consumer with specific reasons why the adverse action was taken."

5. Client shall not request, cause to be prepared or procure an investigative consumer report unless:

a. It is clearly and accurately disclosed to the consumer that an investigative consumer report, may be requested which will include information as to his/her character, general reputation personal characteristics and mode of living, whichever applicable.

6. Client will not use any consumer and/or investigative consumer report prepared by Phillips Agency in violation of any applicable federal or state equal employment opportunity law or regulation.

7. Client shall use the Consumer Report for Employment Purposes only for a one-time use. The report will be held in strict confidence. Client shall not disclose the report to any third party not involved in the employment decision for which the information is sought; provided, however, that User may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. Moreover, unless otherwise explicitly authorized in an agreement between Reseller and its User for scores obtained from

TransUnion, or as explicitly otherwise authorized in advance and in writing by TransUnion through Reseller, User shall not disclose to consumers or any third party, any or all such scores provided under such agreement, unless clearly required by law.

8. Client will maintain a copy of all written authorizations for a minimum of five (5) years from the date of the inquiry.

9. The FCRA provides that any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18 of the United States code or imprisoned not more than two years, or both.

10. Any violation of the terms of this contract or legal requirement or a material change in existing legal requirements that adversely affects the client's agreement, Phillips Agency upon its election with just cause can discontinue serving the client and cancel the agreement immediately.

Subscriber:

Firm/Company/Trade/Individual Name: _____

Management/Corporate/Parent Company Name:_____**Tax**

ID or Social Security #: _____

Address: _____

_____

City: _____**State:** ___**Zip:** _____

Email Address for Billing: _____

Email address for results: _____

Send Invoice by: Email Fax

Telephone #: _____**Fax #:** _____

I agree that I am responsible and/or authorized to bind my company/firm to the charges for services we use. In addition I may be personally held responsible for charges that are not allowed by my company or fraudulently used on behalf of myself or the company's failure to abide by agreement for services. A credit report, criminal report, and/or other sources may be accessed for verification purposes. I also agree to the terms set forth under the section labeled "Certification to Phillips Agency, Inc."

Authorized Agent/Officer Signature:

Print: _____

Title: _____