Third Vision Background Searches
500 N. Michigan Ave Suite 600
Chicago, Illinois 60611
312-396-4002 or 815-669-0556
info@thirdvisionbackgrounds.com

TERMS OF SERVICE/END USER AGREEMENT

THIS END-USER AGREEMENT ("Agreement") is made and entered into by and between Third Vision Background Searches, LLC (its parent, subsidiaries, predecessors, successors, affiliates, directors, officers, fiduciaries, insurers, employees and agents (jointly, "Third Vision Background Searches, LLC") and End-User (its parent, subsidiaries, predecessors, successors, affiliates, directors, officers, fiduciaries, insurers, employees and agents (jointly "End-User"). This Agreement shall be effective on the date of signature below (the "Effective Date").

General

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

End-User's Certification of Fair Credit Reporting Act (FCRA) Permissible Purpose(s)

End-User hereby certifies that all of its orders for information products from Third Vision Background Searches, LLC 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:

(Please check one. Typically, the first and third are common for tenant screening purposes and the second is for employment screening purposes.)

[ ]	Section 604(a)(2). As instructed by the consumer in writing.
[x]	Section 604(a)(3)(B). For employment purposes including evaluating a consumer for employment, promotion, reassignment or retention as an employee, where the consumer has given prior written permission.

[ ]	Section 604(a)(3)(F)(i). Where there is a legitimate business need, in connection with a business transaction that is initiated by the consumer.

Each time End-User makes a request for a report, it is re-certifying the specific permissible purpose listed herein and affirming that if it is for an employment purpose that: A clear and conspicuous stand-alone disclosure, in a document consisting solely of the disclosure, has been made in writing to the consumer. The disclosure satisfied all requirements identified in the Fair Credit Reporting Act and other applicable state laws and that the written authorization of the consumer has been obtained.

End-User's Certification of Legal Compliance

End-User certifies to Third Vision Background Searches, LLC that the information products it receives will not be used in violation of any applicable federal, state or local laws, including, but not limited to the Fair Credit Reporting Act and Title VII of the Civil Rights Act of 1964. End-User accepts full responsibility for complying with all such laws and for using the information products it receives from Third Vision Background Searches, LLC in a legally acceptable fashion. To that end, End-User agrees to comply with and provide all statutorily required notices in Section 615 of the Fair Credit Reporting Act or other state laws when using information products. End-User further accepts full responsibility for any and all consequences of use and/or dissemination of those products. End-User further agrees that each consumer report will only be used for a one- time use.

End-User agrees to have 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 all consumer report or investigative consumer report information including, for example, restricting terminal access, utilizing passwords to restrict access to terminal devices, and securing access to and dissemination of electronic and hard copy reports. End User agrees to securely destroy all hard copy documents and electronic media which may contain private consumer information in accordance with the FTC document destruction requirements. End User also agrees to abide by Addendum A attached hereto which is incorporated into and is part of this Agreement.

As a condition of entering into this Agreement, End-User certifies that it has in place reasonable procedures designed to comply with all applicable local, state and federal laws. End-User also certifies that it will retain any information it receives from Third Vision Background Searches, LLC for a period of five years from the date the report was received, and will make such reports available to Third Vision Background Searches, LLC upon request. End-Users seeking credit information must provide information and acknowledge Addendum B, C, D and E as applicable before Third Vision Background Searches, LLC can provide credit information to End-User. End-User understands that the credit bureaus require specific written approval from Third Vision Background Searches, LLC before the following persons, entities and/or businesses may obtain credit reports: private detectives, private detective agencies, private investigative companies, bail bondsmen, attorneys, law firms, credit counseling firms, security services, members of the media, resellers, financial counseling firms, credit repair clinics, pawn shops (except companies that do only Title pawn), check cashing companies (except companies that do only loans, no check cashing), genealogical or heir research firms, dating services, massage or tattoo services, businesses that operate out of an apartment, individuals seeking information for their own private use, adult entertainment services of any kind, companies that locate missing children, companies that handle third party repossession, companies seeking information in connection with time shares, subscriptions companies, individuals involved in spiritual counseling or persons or entities that are not an End-User or decision maker.

(i) Civil Code Sections 1785.11 and 1786.12.

(ii) When, at any time, Information Products are sought for employment purposes other than suspicion of wrongdoing or misconduct by the consumer who is the subject of the investigation, provide a clear and conspicuous disclosure in writing to the consumer, which solely discloses: (1) that an investigative Information Products may be obtained; (2) the permissible purpose of the investigative Information

Products; (3) that information on the consumer's character, general reputation, personal characteristics and mode of living may be disclosed; and (4) the name, address, telephone number, and website of the Consumer Reporting Agency conducting the investigation; and (5) the nature and scope of the investigation requested, including a summary of the provisions of California Civil Code Section 1786.22.

(iii) When, at any time, Information Products are sought for employment purposes other than suspicion of wrongdoing or misconduct by the consumer who is the subject of the investigation, only request an Information Product if the applicable consumer has authorized in writing the procurement of the Information Product.

(iv) When Information Products are sought in connecting with the hiring of a dwelling unit, notify the consumer in writing that an Information Product will be made regarding the consumer's character, general reputation, and personal characteristics. The notification shall include the name and address of End User as well as a summary of the provisions of California Civil Code Section 1786.22, no later than three days after the date on which the Information Product was first requested.

(v) When Information Products are sought in connection with the underwriting of insurance, clearly and accurately disclose in writing at the time the application form, medical form, binder, or similar document is signed by the consumer that an Information Product regarding the consumer's character, general reputation, personal characteristics, and mode of living may be made, or, if no signed application form, medical form, binder, or similar document is involved in the underwriting transaction, the disclosure shall be made to the consumer in writing and mailed or otherwise delivered to the consumer not later than three days after the report was first requested. The disclosure shall include the name and address of End User, the nature and scope of the investigation requested, and a summary of the provisions of California Civil Code Section 1786.22.

(vi) Provide the consumer a means by which he/she may indicate on a written form, by means of a box to check, that the consumer wishes to receive a copy of any Information Products that are prepared.

(vii) If the consumer wishes to receive a copy of the Information Products, the End User shall send (or contract with another entity to send) a copy of the Information Product to the consumer within three business days of the date that the Information Product is provided to End User. The copy of the Information Product shall contain the name, address, and telephone number of the person at End User who issued the report and how to contact him/her.

(viii) Under all applicable circumstances, comply with California Civil Code Sections 1785.20 and 1786.40 if the taking of adverse action is a consideration, which shall include, but may not be limited to, advising the consumer against whom an adverse action has been taken that the adverse action was based in whole or in part upon information contained in the Information Product, informing the consumer in writing of End User's name, address, and telephone number, and provide the consumer of a written notice of his/her rights under the ICRA and the CCRAA.

(ix) Comply with all other requirements under applicable California law, including, but not limited to any statutes, regulations and rules governing the procurement, use and/or disclosure of any Information Products, including, but not limited to, the ICRA and CCRAA.

End-User hereby acknowledges that it has received a copy of the Summary of Rights (16 C.F.R. Part 601, and Notice to Users of Consumer Reports (16 C.F.R. Part 601).

A. <u>When Information Products are Used for Employment Purposes</u>

If the information products End-User obtains from Third Vision Background Searches, LLC 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, has been made in writing to the consumer explaining that a consumer report and/or investigative consumer report may be obtained for employment purposes. This disclosure satisfies all requirements identified in Section 606(a)(1) of the FCRA, as well as any applicable state or local laws and the consumer has authorized, in writing, the obtaining of the report by End-User. End-User certifies that each time it orders a report, it is reaffirming the above certification.

If the consumer is denied employment, or other adverse employment action is taken based in whole or in part on the information products provided by Third Vision Background Searches, LLC End-User will provide to the consumer: (1) a preliminary adverse action notice, and (2) a copy of the report, and (3) a description, in writing, of the rights of the consumer entitled: "A Summary of Your Rights Under the Fair Credit Reporting Act." After the appropriate waiting period, End-User will issue to the consumer notice of the adverse action taken, including the statutorily required notices identified in Section 615 of the Fair Credit Reporting Act.

B. Investigative Consumer Reports

In addition to the disclosure requirements identified above, 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) Third Vision Background Searches, LLC contact information, including complete address and toll-free telephone number. This information will be provided to the consumer no later than five (5) days after the request for such disclosure was received from the consumer or such report was first requested, whichever is the latter.

C. International Criminal Record Searches

End-User understands that searches of international background screening will be conducted through the services of a third-party independent contractor. Because of differences in foreign laws, language, and the manner in which foreign records are maintained and reported, Third Vision Background Searches, LLC cannot be either an insurer or a guarantor of the accuracy of the information reported. End-User therefore releases Third Vision Background Searches, LLC and its affiliated companies, officers, agents, employees, and independent contractors from any liability whatsoever in connection with erroneous information received as a result of an international background screening report.

D. National/Multi-State Database Searches

Third Vision Background Searches, LLC recommends that End-User screen its applicants or employees at the county, state or federal levels. End-User understands that if it chooses not to conduct searches at these levels, Third Vision Background Searches, LLC cannot be held responsible for any records that exist that are not included in the End-User's coverage requested. End- User further understands that the multi- state/nationwide database report will only be offered in conjunction with a county or state-wide government agency criminal search if a hit is found.

E. Verification Services

Third Vision Background Searches, LLC will make a minimum of 3 solid attempts over 3 business days to obtain the verification. If verification is not completed as a result of these attempts, verification may be closed out as incomplete. End-User understands incomplete verification are still billable at the prevailing rate. A solid attempt is defined as a phone call, fax, email or other message to the target regardless whether or not the contact results in a successful message or dialogue. For employment verifications, Third Vision Background Searches, LLC work product will typically contain the dates of service, reason for leaving, job title, eligibility for rehire, contact name, contact title and contact phone number. For education verifications, Third Vision Background Searches, LLC work product will typically contain the dates of attendance, major study, degree obtained and date degree was conferred. Third Vision Background Searches, LLC will also create specialized verification inquiries based on your specific needs.

End-User understands any third-party fees incurred as a result of the verification process, such a data clearinghouse fees, are passed on to End-User in addition to the standard verification charge.

Additional Requirements for Motor Vehicle Records (MVRs) and Driving Records

End-User hereby certifies that Motor Vehicle Records 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 shall be transmitted to Third Vision Background Searches, LLC 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 any other THIRD VISION BACKGROUND SEARCHES, LLC TERMS OF SERVICE / END-USER AGREEMENT

Warrants

In the course of completing background checks, Third Vision Background Searches, LLC may uncover active arrest warrants which are outstanding against the subject. In these cases, Third Vision Background Searches, LLC may be contacted by the law enforcement agency seeking the subject. Subscriber understands that Third Vision Background Searches, LLC will furnish to law enforcement any information contained within the subject's file to assist in the apprehension of the subject. Additionally, Third Vision Background Searches, LLC may contact Subscriber, and Subscriber agrees to release to Third Vision Background Searches, LLC, any and all information Subscriber may have which will further the apprehension of the wanted individual.

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. End-User may not assign or transfer this Agreement without the prior written consent of Third Vision Background Searches, LLC. 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, Florida law shall guide the interpretation of this Agreement, if such interpretation is required. All litigation arising out of this Agreement shall be commenced in Colorado**,** 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 Third Vision Background Searches, LLC. 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 Third Vision Background Searches, LLC 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 Third Vision Background Searches, LLC, to audit its records at any time, upon reasonable notice given. Breaches of this Agreement and/or violations of

applicable law discovered by Third Vision Background Searches, LLC, may result in immediate suspension and/or termination of the account, legal action and/or referral to federal or state regulatory agencies.

Confidentiality

Neither party shall reveal, publish or otherwise disclose any Confidential Information to any third party without the prior written consent of the other party. "Confidential Information" means any and all proprietary or secret data; sales or pricing information relating to either party, its operations, employees, products or services; and, all information relating to any customer, potential customer, Agent, and/or independent sales outlet. The Parties agree to keep this information confidential at all times during the term of this Agreement, and continuing for five years after receipt of any Confidential Information. Notwithstanding anything to the contrary herein, in no event shall Third Vision Background Searches, LLC be required to destroy, erase or return any consumer reports or applicant data related thereto in Third Vision Background Searches, LLC files, all of which Third Vision Background Searches, LLC shall maintain as a consumer reporting agency in strict accordance with all applicable federal, state, and local laws.

Pass Through Clause

In the event, it becomes necessary to share or disclose the contents of any consumer report or investigative consumer report with a third party, no such disclosure shall occur without first obtaining a Certification of Use attached as Addenda H from the receiving party which outlines their obligations with regard to the use of confidential information. Additionally, a written authorization from the applicant consenting to the disclosure must be obtained prior to any release of information. Unsecured means.

Independent Contractor

The parties agree that the relationship of the parties created by this Agreement is that of independent contractor and not that of employer/employee, principal/agent, partnership, joint venture or representative of the other. Except as authorized hereunder, neither party shall represent to third parties that it is the employer, employee, principal, agent, joint venture or partner with, or representative of the other party.

Fees and Payment

End-User agrees to pay nonrefundable fees and other charges or costs for Third Vision Background Searches, LLC background check services. Any charges or costs, including but not limited to surcharges and other fees levied by federal, state, county, other governmental agencies, educational institutions, employer verification lines and licensing agencies, incurred by Third Vision Background Searches, LLC in servicing End- User, will be passed onto End-User. At Third Vision Background Searches, LLC option, payments not received thirty (30) days after the date of the invoice may 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 Third Vision Background Searches, LLC Accounts Payable Department. Accounts with invoices unpaid thirty (30) days or more will be assessed an interest charge of 1 ½ % per month, as allowed by applicable law. A $20.00 fee will be assessed for all returned checks. 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 Third Vision Background Searches, LLC represents a legal authorization to debit the card for the orders placed or for non-payment per the 15-day terms. End-User agrees that prices for services are subject to change without notice, although Third Vision Background Searches, LLC 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 Third Vision Background Searches, LLC.

Warranties and Remedies

End-User understands that Third Vision Background Searches, LLC 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".
Third Vision Background Searches, LLC 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; Third Vision Background Searches, LLC expressly disclaims any and all such representations and warranties.

In addition to any other limitation of liability set forth in this Agreement, Third Vision Background Searches, LLC 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 Third Vision Background Searches, LLC has been advised of the possibility of such damages. End- User shall indemnify, defend and hold harmless Third Vision Background Searches, LLC from and against any and all claims, suits, proceedings, damages, costs, expenses (including, without limitation, reasonable attorneys' fees and court costs) brought or suffered by any third party arising or resulting from, or otherwise in connection with information products provided by Third Vision Background Searches, LLC, any breach by End-User of any of its representations, warranties, or agreements in this Agreement or its negligence or willful misconduct.

Third Vision Background Searches, LLC nevertheless agrees to indemnify End-User and be responsible for actual damages to the extent allowed by law for third party claims directly resulting from Third Vision Background Searches, LLC sole negligence in assembling the consumer report. In the event that Third Vision Background Searches, LLC is determined by a court of competent jurisdiction to be liable to End-User for any matter arising under or relating to this Agreement, whether arising in contract, equity, tort or otherwise (including without limitation any claim for negligence) the amount of damages recoverable against Third Vision Background Searches, LLC for all such matters, will not exceed, in the aggregate, the amount paid to Third Vision Background Searches, LLC by End-User for the service to which a given claim relates provided pursuant to this Agreement, and recover of the amount is End-User's sole and exclusive remedy hereunder.

Third Vision Background Searches, LLC does not guarantee End-User's compliance with all applicable laws in its use of reported information, and does not provide legal or other compliance related services upon which End-User may rely in connection with its furnishing of reports. End-User understands that any conversation or communication with Third Vision Background Searches, LLC representatives regarding searches, verifications or other services offered by Third Vision Background Searches, LLC are not to be considered a legal opinion regarding such use. End-User agrees that it will consult with its own legal or other counsel regarding the use of background screening services, including but not limited to, the legality of using or relying on reported information, development of internal policies and procedures, and adverse action processes.

Term and Termination

The term of this Agreement shall begin on the date it is executed by End-User and shall be in effect for one (1) year beginning on the first day of the assigned date below and renewed automatically for one (1) year each year on its anniversary date, if no written notice is received by either party within thirty (30) days prior to end of term.

Either party may cancel this Agreement by giving sixty (60) day written notice to the other party. Third Vision Background Searches, LLC 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 or other responsibilities and agreements made.

In addition to any and all other rights a party may have available according to law, if a party defaults by failing to

perform any provision, term or condition of this Agreement the other party may terminate the Agreement by providing written notice to the defaulting party. This notice shall describe with sufficient detail the nature of the default. The party receiving such notice shall have fifteen (15) days from the receipt of such notice to cure the default(s). Unless waived by party providing notice, the failure to cure the default(s) within such time period. shall result in the automatic termination of this Agreement.

Force Majeure

End-User agrees that Third Vision Background Searches, LLC is not responsible for any events or circumstances beyond its control (e.g., including but not limited to war, riots, embargoes, strikes and/or Acts of God) that prevent Third Vision Background Searches, LLC from meeting its obligations under this Agreement.

Severability

If any provision of this Agreement, or the application thereof to any person or circumstance, shall be held invalid or unenforceable under any applicable law, such invalidity or unenforceability shall not affect any other provision of this Agreement that can be given effect without the invalid or unenforceable provision, or the application of such provision to other persons or circumstances, and, to this end, the provisions hereof are severable.

Execution

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 individuals signing below represent that they are duly authorized to do so.

ADDENDUM A

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. <u>Implement Strong Access Control Measures</u>

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

1.2 Proprietary or third-party system access software must have credit reporting agency Subscriber Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.

1.3 You must request your Subscriber Code password be changed immediately when:
- any system access software is replaced by system access software or is no longer used;
- the hardware on which the software resides is upgraded, changed or disposed of

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

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

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

1.7 Keep user passwords Confidential.

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

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

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

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

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

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

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

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

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

2. <u>Maintain a Vulnerability Management Program</u>

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. <u>Protect Data</u>

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. <u>Maintain an Information Security Policy</u>

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. <u>Build and Maintain a Secure Network</u>

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. <u>Regularly Monitor and Test Networks</u>

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.

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."

Glossary

Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way acomputer 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	Encryption is 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. Insimpler 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.
Subscriber Code	Your seven-digit credit reporting agency account number.
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. Older technology reaching its end of life.
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).

Company Name_____

Printed Representatives Name_____

Signature(s)_____

Title_____

Address_____ City_____ State_____ Zip code_____

Date_____

Third Vision Background Searches, LLC

Signature of Representative_____

Printed Name_____

Title_____

Date_____