SCOTT•ROBERTS
AND ASSOCIATES, LLC

SERVICE AGREEMENT

This Service Agreement ("Agreement") is hereby entered into by and between Scott-Roberts and Associates, LLC, a Florida corporation ("Scott-Roberts and Associates, LLC"), located at 2290 10th Ave. N., Lake Worth, FL 33461 and the entity indicated on the last page of the Agreement ("Client").

Whereas, Scott-Roberts and Associates, LLC has access to consumer information, including information from one or more consumer credit reporting agencies, as well as access to public records; and **Whereas**, Client has a need for consumer information in connection with either the evaluation of individuals for employment, promotion, reassignment or retention as an employee ("Employment Purposes") or in connection with the evaluation of individuals for tenant leasing/ownership occupancy ("Tenant/Owner Purposes") and wishes to have Scott-Roberts and Associates, LLC prepare consumer reports and/or investigative consumer reports containing information regarding such individuals, as set forth herein; and **Whereas**, Scott-Roberts and Associates, LLC wishes to supply such reports under the terms and conditions set forth herein; and **Whereas**, Scott-Roberts and Associates, LLC and Client agree to comply with all applicable state and federal laws regarding the provision and use of consumer information for Employment Purposes or Tenant/Owner Purposes including, but not limited to, the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §1681 et seq.;

Therefore, in consideration of the terms and conditions set forth herein, the parties agree as follows:

1. **Services Provided.** Scott-Roberts and Associates, LLC agrees to provide information to Client for a permissible purpose under the Fair Credit Reporting Act ("FCRA") and other federal and state laws. As allowed by law and to the extent requested by Client, Scott-Roberts and Associates, LLC may provide the following types of information to Client: credit information, motor vehicle records and driver's license information, criminal records, civil court records, worker compensation records, social security verifications, education records, military records, employment verifications and references and other information related to the consumer's character, general reputation, personal characteristics and mode of living.

2. **Client's Certification of Fair Credit Reporting Act (FCRA) Permissible Purpose(s).** Client hereby certifies that all of its orders for information from Scott-Roberts and Associates, LLC shall be made, and the resulting reports shall be used, for the following permissible purpose under the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, only:

[ ]	For "Employment Purposes," but only upon the express written consent of any person that will be screened. See 15 U.S.C §1681b(a)(3)(B).
[ ]	For "Tenant/Owner Purposes" but only upon the express written consent of any person that will be screened. See 15 U.S.C. §1681b(a)(2).

Client will immediately alert Scott-Roberts and Associates, LLC if it intends to request a report from Scott-Roberts and Associates, LLC for a purpose other than the one specified above.

3. **Client's Certification of Legal Compliance.** Client certifies to Scott-Roberts and Associates, LLC that the information it receives will not be used in violation of any applicable federal, state or local laws. Client accepts full responsibility for complying with all such laws and for using the information it receives from Scott-Roberts and Associates, LLC in a legally acceptable fashion. Client further accepts full responsibility for any and all consequences of use and/or dissemination of those products. PLEASE

NOTE: 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.

As a condition of entering into this Agreement, Client certifies that it has in place reasonable procedures designed to comply with all applicable local, state, and federal laws. Client also certifies that it will retain any information and reports it receives from Scott-Roberts and Associates, LLC for a period of five years from the date the report was received, and will maintain copies of all written authorizations for a minimum of five years.

Client certifies that it shall use any consumer reports or investigative consumer reports: (a) solely for the Client's certified use(s); and (b) solely for Client's exclusive one-time use. Client shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, or renting information obtained under this Agreement to any other party, whether alone, in conjunction with Client's own data, or otherwise in any service which is derived from the consumer reports or investigative consumer reports. Client shall hold any consumer report or investigative consumer report in strict confidence, and not disclose it to any third-parties except as necessary to comply with adverse-action requirements under the Fair Credit Reporting Act or as otherwise required by law.

Client shall ensure that employees shall not attempt to obtain any consumer reports or investigative consumer reports on themselves, associates, or any other person except in the exercise of their official duties. Client certifies that all persons authorized by Client to obtain and/or use reports on behalf of Client will be informed of their obligations under this Agreement. Client will restrict access to information contained in any report to those employees and agents with a legitimate business reason to receive such information.

Clients obtaining credit information from Scott-Roberts and Associates, LLC agree to abide by the document entitled "Access Security Requirements," attached hereto. Likewise, as a condition of entering into this Agreement, Client certifies that it has in place reasonable procedures designed to comply with all applicable local, state and federal laws.

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

Client certifies that prior to obtaining or causing a "consumer report" and/or "investigative consumer report" to be obtained for "Employment Purposes," 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 604(b)(2) and 606(a)(1) of the FCRA, as well as any applicable state or local laws. The consumer will authorize, in writing, the obtaining of any report by Client from Scott-Roberts and Associates, LLC for "Employment Purposes."

If the consumer may be denied employment or incur another adverse action based in whole or part on a report provided by Scott-Roberts and Associates, LLC, Client 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." After the appropriate waiting period, Client will issue to the consumer notice of the adverse action taken, including the statutorily-required notice identified in Section 615 of the Fair Credit Reporting Act. Among other things, such notice will include: (1) the name, address, and telephone number of consumer reporting agency Scott-Roberts and Associates, LLC, (2) a statement that the consumer reporting agency did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken, (3) a statement that the

consumer may obtain a free copy of the consumer report from the consumer reporting agency within 60 days pursuant to Section 612 of the Fair Credit Reporting Act, and (4) a statement that the consumer has the right to dispute with the consumer reporting agency the accuracy or completeness of any information in a consumer report furnished by the agency.

Client hereby acknowledges that it has received a copy of the Summary of Rights (16 C.F.R. Part 601, Appendix A) and Notice of Users of Consumer Reports (16 C.F.R. Part 601, Appendix C).

Client also acknowledges that it is aware that local, state, and federal laws and regulations impact how and under what circumstances Client may use criminal history information, credit history information, and other consumer report information. Client assumes full responsibility for complying with all applicable laws and regulations. Among other things, Client has or will become familiar with April 2012 EEOC Enforcement Guidance explaining how employers may utilize criminal history information in compliance with Title VII of the Civil Right Acts of 1964, as amended.

B. When Reports Are Used For Tenant/Owner Purposes.

If Client intends to request a report from Scott-Roberts and Associates, LLC for "Tenant/Owner Purposes," it will first obtain the written consent of the consumer to do so.

If Client takes adverse action against a tenant or prospective tenant based upon a consumer report or investigative consumer report from Scott-Roberts and Associates, LLC, Client agrees to follow all adverse action requirements specified in Section 615 of the Fair Credit Reporting Act. Among other things, Client agrees that after taking adverse action it will provide a notice to the consumer that includes: (1) the name, address, and telephone number of consumer reporting agency Scott-Roberts and Associates, LLC, (2) a statement that the consumer reporting agency did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken, (3) a statement that the consumer may obtain a free copy of the consumer report from the consumer reporting agency within 60 days pursuant to Section 612 of the Fair Credit Reporting Act, and (4) a statement that the consumer has the right to dispute with the consumer reporting agency the accuracy or completeness of any information in a consumer report furnished by the agency.

4. **Investigative Consumer Reports.** Regardless of whether screening is being done in connection with an employment or tenant situation, if the consumer makes a written request within a reasonable amount of time, Client 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) Scott-Roberts and Associates, LLC's 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 is received from the consumer or such report is first requested, whichever is the latter.

5. **Motor Vehicle Records (MVRs) and Driving Records.** Regardless of whether screening is being done in connection with an employment or tenant situation, Client 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. Client further certifies that no MVRs shall be ordered without first obtaining the written consent of the consumer to obtain "driving records." Client 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. Client shall not transmit any data contained in the resulting MVR via the public internet, electronic mail or any other unsecured means.

6. **National/Multi-State Database Searches.** Regardless of whether screening is being done in connection with an employment or tenant situation, Scott-Roberts and Associates, LLC recommends that Client screen individuals at the following levels: county court-house (or online system), federal, and multi-state/nationwide database levels. Client understands that if it chooses not to conduct searches at these levels, Scott-Roberts and Associates, LLC cannot be held responsible for any records that exist that are not included in the Client's coverage requested. Client further understands that the multi-state/nationwide database report will only be offered in conjunction with a county-level verification of any records found, and that Client will bear any additional costs associated with this verification.

7. **Credit Scores.** To the extent Client is eligible to receive credit scores ("Scores"), Client will request them only for Client's exclusive use. Client may store scores solely for Client's own use in furtherance of Client's original purpose for obtaining the scores. Client shall not use the scores for model development or model calibration and shall not reverse engineer the score. All scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part to any person except: (i) to those employees of Client with a need to know and in the course of their employment; (ii) to those third party processing agents of Client who have executed an agreement that limits the use of the scores by the third party to the use permitted to Client and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering; (iii) when accompanied by the corresponding reason codes to the consumer who is the subject of the score; or (iv) as required by law.

8. **Confidentiality.** Except as required by law, Scott-Roberts and Associates, LLC will use its best efforts to maintain the confidentiality of Client's screening requests, and will not divulge the information obtained on Client's behalf nor the contents of any report prepared on Client's behalf, to any person other than the Client and the subject of the report.

9. **Billing.** Scott-Roberts and Associates, LLC will send an invoice to Client monthly for all services performed. Invoices are due upon receipt. Any payment not received by Scott-Roberts and Associates, LLC within thirty (30) days of invoice date shall be deemed past due. To the extent permitted by law, a service and interest charge of 1.5% shall be added to all invoices on the thirty-first day following the invoice date, and each thirty days thereafter. Scott-Roberts and Associates, LLC reserves the right to suspend services due to non-payment. Client acknowledges that if formal collection efforts are required by Scott-Roberts and Associates, LLC to collect unpaid balances from Client, Client will pay reasonable attorney's fees and costs associated with such collection efforts.

10. **Term.** Either party may cancel this Agreement at any time, with or without cause, upon written notice to the other. Scott-Roberts and Associates, LLC, at its option, may complete any or all services requested as of the time of cancellation or, may notify Client that it will not complete such services. Client agrees to pay for all services requested by Client prior to cancellation of this Agreement, and which are actually completed by Scott-Roberts and Associates, LLC. Should Client require cancellation of a particular consumer report after sending report request but before receiving report, Client agrees to pay for all services in process at time of request to cancel. Client recognizes and agrees that violation of the Agreement, including misuse of information obtained pursuant to this Agreement, or violation of any law or regulation, shall be cause for immediate termination of this Agreement by Scott-Roberts and Associates, LLC and will result in cessation of services hereunder.

11. **Warranties and Indemnification.** Scott-Roberts and Associates, LLC assembles information from many sources, including databases maintained by consumer reporting agencies containing information from public records, other information repositories, and third-party researchers. Client understands that these information sources and resources are not maintained by Scott-Roberts and Associates, LLC. Therefore, Scott-Roberts and Associates, LLC cannot be a guarantor that the information provided from

these sources is absolutely accurate or current. Nevertheless, Scott-Roberts and Associates, LLC has in place procedures designed to respond promptly to claims of incorrect or inaccurate information in accordance with applicable law.

Client understands that Scott-Roberts and Associates, LLC obtains the information in its reports from various third party sources "AS IS" and, therefore, is providing the information to Client "AS IS". Scott-Roberts and Associates, 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 and/or consumer reports, that the reports will meet Client's needs or will be provided on an uninterrupted basis; Scott-Roberts and Associates, LLC expressly disclaims any and all such representations and warranties.

Client agrees to indemnify, defend, and hold harmless Scott-Roberts and Associates, LLC, its successors and assigns, officers, directors, employees, agents, vendors, and suppliers from any and all third-party claims, actions or liabilities arising from or with respect to: (i) any breach by Client of this Agreement or the representations, certifications or warranties made hereunder, (ii) Client's violation of applicable laws or ordinances, (iii) Client's negligence, misconduct, recklessness, errors or omissions, or (iv) Client's acquisition of or use of Scott-Roberts and Associates, LLC's reports or services.

Scott-Roberts and Associates, LLC does not guarantee Client's compliance with all applicable laws in its use of reported information and does not provide legal or other compliance-related services upon which Client may rely. Client understands that Scott-Roberts and Associates, LLC is not a law firm and that any documents, communications or information received from Scott-Roberts and Associates, LLC regarding the obtainment or use of background screening reports is not to be considered legal counsel or legal opinion. Client agrees that it will consult with its own legal counsel regarding the acquisition and use of background screening information, including but not limited to, the legality of using or relying on reported information and the appropriate procedure for taking adverse action based upon a consumer report and/or investigative consumer report.

12. **Remedies.** Scott-Roberts and Associates, LLC's liability for alleged damages to client will be limited to the amount of actual damages incurred by Client, provided however, that in no event will Scott-Roberts and Associates, LLC's aggregate liability hereunder exceed three (3) times the average monthly fee paid by Client to Scott-Roberts Associates for screening services during the year in which the claim arose. IN NO EVENT WILL EITHER PARTY BE RESPONSIBLE FOR SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR OTHER SIMILAR DAMAGES IN CONNECTION WITH THE SCREENING SERVICFS, EVEN IF EITHER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Scott-Roberts and Associates, LLC and Client will use reasonable efforts to mitigate any potential damages or other adverse consequences arising from or related to the screening services. Nothing in this Agreement is intended to limit either party's obligation to mitigate damages. The parties acknowledge that the fees for the screening services to be provided under this Agreement reflect the allocation of risk as set forth in this section. This section sets forth the full extent of Client's remedies against Scott-Roberts and Associates, LLC.

13. **E-Services.** Client agrees that, upon request, Scott-Roberts and Associates, LLC will grant access to services through the use of a secure Internet connection. In order to protect against the unauthorized access and improper use of consumer information, Client agrees that:

a) It shall designate a Principle Account User, who shall sign this Agreement.

b) Only persons who have signed a Client Agreement shall have access to Client's Client ID Number or Username information.

c) Each Client will have his or her own password. Client shall promptly notify Scott-Roberts and Associates, LLC of any change in employment status or other reason to restrict access to any Client.

d) Client shall be solely liable for any misuse of information by its employees and/or agents.

14. **Proprietary Rights and Confidentiality.** Client hereby acknowledges and agrees that Scott-Roberts and Associates, LLC's methods, means and processes for collecting, decoding, assembling, assessing and conveying its services constitute proprietary information. Client hereby agrees to exercise due and reasonable care in protecting Scott-Roberts and Associates, LLC's confidential information from unauthorized use or disclosure.

15. **Force Majeure.** Scott-Roberts and Associates shall not be responsible for any delay or failure to perform under this Agreement for reasons of war, insurrection, riot, power failure or others circumstances beyond Scott-Roberts and Associates' reasonable control. In case of errors or lost data caused by power failure, mechanical difficulties with information storage and retrieval systems, or other events not attributable to its own negligence or willful misconduct, Scott-Roberts and Associates sole obligation will be to use its reasonable efforts to reconstruct any records maintained by Scott-Roberts and Associates and to amend any reports prepared by it with may have been affected by such event, at its own expense.

16. **Choice of Law.** This Agreement shall be governed by the laws of the State of Florida, including all choice of law rules.

17. **Venue.** All litigation arising out of this Agreement shall be commenced in Florida, and the parties hereby consent to such jurisdiction and venue.

18. **Entire Agreement.** The parties hereto agree that this Agreement, and all attachments and appendices hereto, constitute the entire Agreement of the parties regarding the subjects contained herein and supersedes any prior agreements, whether written or oral. This Agreement may only be amended by a written agreement, signed by both parties.

20. **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 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.

21. **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.

22. **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.

CLIENT:

Authorized Agent of Client	Title	Date

SCOTT-ROBERTS AND ASSOCIATES, LCC

Robert Buchholz or Andrew Scott	Date

Client Information

Organization Name		Telephone	Fax
Primary Contact	Title	Telephone	E-mail
Street Address		City, State	ZIP
Company Website URL		EIN#	
Nature of Business			

The following persons are authorized to access the account:

Contact:_____

Contact:_____

Application To Become Client

Date of Application: _____

Important: **All information must be completed in its entirety. Please print clearly and legibly to ensure accurate and timely processing.**

General Company Information

Company Name: _____ Years In Business _____ yrs _____ mos.

Type of Ownership (Indicate one): ☐ Partnership ☐ Sole Owner ☐ Nonprofit ☐ Corporation ☐ LLC

Do you have any other company name(s) or dba? ☐ Yes ☐ No If Yes, please list: _____

Website Address: _____

Physical Street Address (no P.O. box numbers, please): _____

City: _____ State: _____ ZIP: _____ How Long? _____ yrs _____ mos.

Phone: ( ) _____ Fax: ( ) _____ Is this a residential address? ☐ Yes ☐ No

Previous Address: _____

City: _____ State: _____ ZIP: _____ How Long? _____ yrs _____ mos.

Do you own or lease the building in which you are located? (please check one) ☐ **Own** ☐ **Lease**

Principal of the Company

If sole owner or partnership, please complete this section

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

Principal name: _____

Title or Position: _____ Phone: ( ) _____

Social Security Number _____ Year of Birth: _____

Residential Street Address: _____

City: _____ State: _____ ZIP: _____

Affiliated or Parent Company Information

***Do you have any branch offices located in the state of California'?** ☐ **Yes** ☐ **No**

Affiliated or Parent Company Name: _____

Contact Name: _____ **Title:** _____

Address: _____ **Phone:** ( ) _____

City: _____ **State:** _____ **ZIP:** _____

Business Information

(Please tell us about your company.)

Type of Business: _____ Do you need a Purchase Order? ☐ **Yes** ☐ **No** PO# _____

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

Estimated # of Consumer Reports you will access monthly: _____

How will you access the Consumer Reports? ☐ **Personal Computer** ☐ **Credit Terminal** ☐ **CPU-CPU** ☐ **Phone/Fax**

Do you already have a credit reporting software package? ☐ **Yes** ☐ **No** If **Yes,** what is the name? _____

Does your company qualify for sales tax exemptions? ☐ **Yes** ☐ **No** If **Yes,** please provide proof.

Permissible Purpose/Appropriate Use	**(Application will not be processed unless this information is provided.)**

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

NOTE: The response to this question must match the response placed on the Service Agreement.

This section MUST be completed.

Bank Reference (Please provide the name of the bank which maintains your business checking account.)

Bank Name: _____ Phone: ( ) _____

Address: _____

City: _____ State: _____ ZIP: _____

Business Checking Account Number(s): _____

The following applies to companies ordering consumer reports and/or investigative consumer reports.

I have read and understand the **"FCRA Requirements"** notice and **"Access Security Requirements"** and will take all reasonable measures to enforce them within my facility. I certify that I will use the consumer report/investigative consumer report information for no other purpose other than what is stated in the Permissible Purpose/Appropriate Use section on this application and for the type of business listed on this application. I will not resell the report to any third party. I understand that if my system is used improperly by company personnel, or if my access codes are made available to any unauthorized personnel due to carelessness on the part of any employee of my company, I may be held responsible for financial losses, fees, or monetary charges that may be incurred and that my access privilege may be terminated.

_____
Company Name

_____ _____
Type or Print Name of Owner or Officer Title

SIGN X X HERE

_____ _____
Authorized Signature Date

Experian

Access Security Requirements for Resellers of FCRA and GLB 5A Data

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. Experian reserves the right to make changes to Access Security Requirements without notification. The information provided herewith provides minimum baselines for information security.

In accessing Experian's services, you agree to follow these security requirements:

1. **Implement Strong Access Control Measures**

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

   1.2 Proprietary or third party system access software must have Experian 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 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 Experian 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 Experian'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 Experian 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 Experian 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 Experian 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 Experian systems and networks. These controls should be selected and

Experian

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, Experian 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 consumer complaint that your company impermissibly accessed their credit report, Experian 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."

Signature/Title _____ Date _____

Experian

Glossary

Term	Definition
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 your 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. 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.
Subscriber Code	Your seven digit Experian 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).