SCOTT ROBERTS AND ASSOCIATES

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 1601 Forum Pl, Ste 203, West Palm Beach, FL 33401 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

(Please check box below):

☐ 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. **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.**

3) **Client's Certification of Legal Compliance.** Client shall comply with all laws applicable to its request for, receipt of, or use of consumer reports and/or investigative consumer reports. Among other things, Client makes the following certifications:

A. When Reports are Ordered/Used for Employment Purposes.

Client understands that various legal requirements apply when it orders reports for employment purposes. Client shall comply with all such requirements. In particular, Client makes the following certifications as to legal compliance:

I. **Disclosure.** Client certifies that, in compliance with the FCRA, prior to ordering a report, Client shall make a clear and conspicuous "disclosure" in writing to the individual about whom the report will be run ("the Consumer"). The "disclosure" shall explain that a consumer report may be procured for employment purposes. The "disclosure" shall describe the nature of the reports to be ordered, and meet all other requirements specified by applicable law. Among other things, the "disclosure" shall "stand alone" and not be combined with or stapled to any employment application or other document. The "disclosure" shall also not contain any extraneous information not required by applicable law, including, but not limited to, a release of liability.

II. **State Law Notifications.** Client certifies that before ordering a report from Scott-Roberts and Associates, LLC, it shall also provide any necessary notifications under applicable state law to the Consumer. Client understands that various states, including, but not limited to, California, Minnesota, Oklahoma, New York, Massachusetts, and Washington require that specific information be communicated to the Consumer under certain circumstances. Client also understands that certain states, such as California, Oklahoma, and Minnesota, require that applicants/employees be afforded a check box to allow them to indicate that they would like a copy of any report received by Client. Client agrees that it will work with experienced legal counsel as appropriate to ensure that all applicable requirements are accounted for.

III. **Written Consent.** Client certifies that, consistent with the FCRA, before ordering a report, the Consumer shall authorize in writing the procurement of such report.

IV. **EEO Law and Regulation Compliance.** Client certifies that it shall not use information contained in a report provided by Scott-Roberts and Associates, LLC, in violation of any applicable federal or state equal employment opportunity law or regulation.

V. **Adverse Action Procedures.** Client certifies that, if it is contemplating taking adverse action based in part or whole on a report from Scott-Roberts and Associates, LLC, it shall follow all legally-required "adverse action" procedures specified by applicable federal, state and/or local law. For example, 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, (2) a description, in writing, of the rights of the consumer entitled "A Summary of Your Rights Under the Fair Credit Reporting Act," and (3) a written notice containing any and all required notifications under federal, state or local law. Client will then wait a reasonable period of time to allow the Consumer to dispute the accuracy of the report. After the appropriate waiting period and, assuming no dispute, Client will issue to the Consumer notice of any adverse action taken, including the statutorily-required notice identified in the Fair Credit Reporting Act.

VI. Among other things, such notice will include: (1) the name, address, and telephone number of the 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. If a dispute as to the accuracy of the report is raised by the Consumer during the waiting period, Client will afford Scott- Roberts and Associates, LLC, the legally-allowed time to resolve the dispute before deciding whether to take adverse action.

VII. **Certifications Associated With Each Order.** By having Scott-Roberts and Associates, LLC prepare a report for Client, Client is certifying that: (1) A clear and conspicuous disclosure has been made in writing to the Consumer by End- User (in a document that consists solely of the disclosure) stating that a Consumer Report may be obtained for employment purposes; (2) the Consumer has authorized in writing the procurement of the Consumer Report that is being ordered; (3) information from the report to be provided by Scott-Roberts and Associates, LLC will not be used in violation of any applicable Federal or State equal employment opportunity law or regulation, or any other applicable law; and (4) if applicable, End-User will comply with the adverse action requirements described in Section 604(b)(3) of the Fair Credit Reporting Act, as well as any other pertinent adverse action requirements. In addition, if the Consumer lives in California or is applying to work in California or works in California, by having Scott-Roberts and Associates, LLC prepare a report for Client, Client is certifying that: (1) Client has complied with all disclosure and authorization requirements set forth in California Civil Code 1786.16, (2) Client has provided the Consumer a means to check a box to indicate that he or she would like a copy of any report received by Client from Scott-Roberts and Associates, LLC, (3) Client will comply with any adverse requirements set forth under California law (including those identified in Section Cal. Civ. 1786.40) should they become applicable, and (4) Client has otherwise met all requirements for obtaining a consumer report or investigative consumer report under California law.

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

If Client intends to request a report from Scott-Roberts and Associates, LLC for "Tenant/Owner Purposes," Client certifies as follows:

I. **Federal, State, and Local Law Notifications.** Client certifies that before ordering a report from Scott-Roberts and Associates, LLC, for Tenant/Owner Purposes, it shall provide any necessary notifications under applicable federal, state, and local law to the Consumer. Client understands that various states, including, but not limited to, California, New York, Massachusetts, and Washington require that specific information be communicated to the Consumer under certain circumstances. Client agrees that it will work with experienced legal counsel as appropriate to ensure that all applicable requirements are accounted for.

II. **Written Consent.** Client certifies that, consistent with the FCRA, before ordering a report from Scott-Roberts and Associates, LLC, the Consumer shall authorize in writing the procurement of such report. Consent paperwork shall appropriately inform the Consumer of the tenant-related reason for the Scott-Roberts and Associates, LLC check and the nature of such check, in compliance with the FCRA.

III. **Post-Adverse Action Procedures.** If Client decides to take adverse action based upon a report provided by Scott-Roberts and Associates, LLC (e.g., decline tenant application, require higher security deposit, or offer less desirable apartment), it shall issue to the Consumer notice of any adverse action taken based in part or whole on a report, including the statutorily-required notice identified in the Fair Credit Reporting Act. Among other things, such notice shall include: (1) the name, address, and telephone number of the 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, Client certifies that it shall comply with additional requirements pertaining to investigative consumer reports, as outlined in 15 U.S.C. § 1681d, if applicable. Among other things, it shall clearly and accurately disclose to the Consumer that an investigative consumer report, including information as to his/her character, general reputation, personal characteristics, and mode of living, whichever are applicable, may be obtained. The disclosure shall be made in writing and mailed or otherwise delivered to the Consumer with a summary of the Consumer's rights provided for under 15 U.S.C. § 1681g(c). The disclosure shall also include a statement informing the Consumer of his/her right to submit a written request for additional information, pursuant to 15 U.S.C. § 1681d(b), within a reasonable period of time after the receipt by him/her of the foregoing disclosure. By having Scott-Roberts and Associates, LLC prepare an investigative consumer report for Client, Client is certifying that it has complied with the above requirements in this Section and otherwise met all legal prerequisites for receiving an investigative consumer report. Further, upon receipt of a request by a consumer for additional information about the investigative consumer report being ordered, Client shall disclose in writing the nature and scope of the investigation, which shall be complete and accurate. The disclosure must be mailed or otherwise delivered to the Consumer not later than five (5) days after the date on which the request for additional disclosure was received from the Consumer or the date the Client first requested the report, whichever is later.

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 internet, electronic mail or any other unsecured means.

6) **Criminal History 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 multistate/nationwide database levels. Client understands that it shall not receive any criminal records that fall outside of its requested searches. 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. Finally, Client is aware that multiple states and municipalities impose restrictions on the use of criminal history information and that the EEOC counsels that employers should engage in a multi-step process when evaluating applicants'/employees' criminal

history information designed to avoid any disparate impact problems under Title VII. Client agrees to monitor all applicable legal restrictions on the use of criminal history information and take all necessary steps to comply with them.

7) **The Work Number.** Client acknowledges that special requirements are imposed by "The Work Number" before access to "The Work Number" may be provided by Scott-Roberts and Associates, LLC. If Client chooses to order such information from Scott-Roberts and Associates, LLC, Client agrees as follows:
   a) Client shall hold "The Work Number" and its agents harmless from any claims or injuries arising out of Client's use of "The Work Number."
   b) Client shall not forward or share "The Work Number" information with any third-party, except as required by law.
   c) "The Work Number" information will only be obtained by Client for the permissible purpose identified in this Agreement.
   d) Client is not one of the companies identified by "The Work Number" as a "Business that Cannot Be Provided The Work Number Information."
   e) Client is in compliance with Florida laws and/or other applicable state laws regarding consumer credit or consumer identity protection.
   f) Client shall comply with "The Work Number" data security requirements and "The Work Number's" disposal of consumer information requirements.

8) **Credit Information.** If Client chooses to order credit reports from Scott-Roberts and Associates, LLC, it certifies the following:
   a) If Client is an employer, Client understands that at least ten (10) states and certain municipalities impose requirements and/or restrictions on employers intending to use credit reports for employment purposes. For example, Nevada and Illinois only permit employers to consider credit reports if the Consumer is working or will be working in a certain capacity. Likewise, states such as California and Colorado require that Consumers receive certain additional notifications before a credit check for employment purposes is conducted. Client certifies that it will comply with any and all legal requirements or restrictions pertaining to its use of credit reports identified by Scott- Roberts and Associates, LLC.
   b) Client acknowledges that special requirements are imposed by credit bureaus before access to credit history information may be provided. Client therefore agrees to the following:
   i. Client shall make no employment decisions based solely on credit bureau alerts/warnings regarding addresses and/or Social Security numbers.
   ii. Client shall permit a physical site inspection of its premises. The cost for the site inspection will be billed to Client. Scott-Roberts and Associates, LLC will arrange for an inspector to come to Client's location. For residential offices, the inspection and fee will be annual.
   iii. Client shall ensure security programs and appropriate access requirements are in place, the purpose being to prevent unauthorized ordering, accessing, and/or unauthorized viewing of consumer information; to inform all accessing employees that they may not access their personal information, information of friends and/or relatives or any other person unless it is for legitimate business purposes.
   iv. To the extent Client is eligible to receive credit scores ("Scores"), Client shall only do so for its own 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 by Client 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 and other contractors of Client who have executed an agreement that limits the use of the Scores by the third party only to the use permitted to Client and contains the prohibitions 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. Moreover, unless otherwise explicitly authorized in an agreement between Scott-Roberts and Associates, LLC and Client for scores obtained from a credit bureau, or as explicitly otherwise authorized in advance and in writing by a credit bureau through Scott-Roberts and Associates, LLC, Client shall not disclose to consumers or any third party, any or all such scores provided under this Agreement, unless required by law.
   v. Client shall release and indemnify the credit reporting agency from all liability arising from the Client's unauthorized access, improper use, or reliance on consumer credit information provided by the Company pursuant to this agreement.
   vi. Client shall comply with any other requirement imposed by a credit reporting agency, so long as Scott-Roberts and Associates, LLC, makes Client aware of such a requirement.

9) **Client's Information Security Obligations.** Client understands that reports contain sensitive, personal information. Accordingly, Client agrees to do the following to preserve the security of the information being provided pursuant to this Agreement:

A. **Prevent Misuse Of Services Or Information.** Client shall only request reports for one-time use and for the permissible purpose(s) identified in this Agreement. Client agrees to take appropriate measures to protect against the misuse and/or unauthorized access of reports. Client agrees that Scott-Roberts and Associates, LLC may temporarily suspend Client's access pending an investigation of Client's use or access. Client agrees to cooperate fully with any and all investigations. If any misuse or unauthorized access is found, Scott-Roberts and Associates, LLC, may immediately terminate this Agreement. Client is solely responsible for any misuse of services or information by its employees and/or agents.

B. **Properly Maintain The Client Account.** Upon request, Scott-Roberts and Association, LLC, will grant access to services through the use of a secure Internet connection. Client shall designate a Principal Account user, who shall sign this Agreement. Only persons who have signed a Client Agreement shall have access to Client's Client ID Number or Username information. Client is responsible for the administration and control of its Client ID Numbers or Usernames by its employees and third parties and shall identify a security administrator to coordinate with Scott-Roberts and Associates, LLC. Client shall manage all ID Numbers and Usernames and notify Scott-Roberts and Associates, LLC, promptly if any ID Number or Username becomes inactive or invalid or if there is another reason to restrict access to Client. Client shall follow the policies and procedures of Scott-Roberts and Associates, LLC, with respect to account maintenance as communicated to Client from time to time.

C. **Limit Access Within Organization**. Client shall disclose reports internally only to Client's designated and authorized employees having a need to know and only in accordance with the Agreement and applicable law. Client shall ensure that such designated and authorized employees shall not attempt to obtain any consumer reports or investigative consumer reports on themselves, associates, or any other person except in the reasonable exercise of their official duties.

D. **Limit Distribution Outside of Organization**. Client shall hold any report obtained from Scott-Roberts and Associates, LLC, 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.

E. **Properly Handle Any Potential Or Actual Security Breaches.** In the event that Client learns or has reason to believe that report data has been disclosed or accessed by an unauthorized party, Client will immediately give notice of such event to Scott-Roberts and Associates, LLC. Furthermore, in the event that Client has access to or acquires individually- identifiable information (e.g., social security numbers, driver's license numbers or dates of birth) in relation to the Agreement, the following shall apply: Client acknowledges that upon unauthorized acquisition of such individually-identifiable information (a "Security Event"), Client shall, in compliance with law, notify the individuals whose information was disclosed that a Security Event has occurred. Also, Client shall be responsible for any other legal obligations which may arise under applicable law in connection with such Security Event.

F. **Deletion.** When Client disposes of consumer reports, investigative consumer reports, and/or other background screening-related documents containing personally identifiable information, it will do so in a safe manner that comports with the Fair Credit Reporting Act and Driver Privacy Protection Act ("DPPA" at 18 U.S.C. § 2721 et seq.). For example, so long as permissible under the law, Client will burn, pulverize, or shred hard copies of such documents rather than place them in a waste basket or recycle bin.

G. **Comprehensive Information Security Program.** Client certifies that they shall implement and maintain a comprehensive information security program written in one or more readily accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to the client's size and complexity, the nature and scope of its activities, and the sensitivity of the information provided to the client by Scott-Roberts and Associates, LLC; and that such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonably designed to (i) insure the security and confidentiality of the information provided by Reseller, (ii) protect against any anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any consumer.

H. Access to the Death Master File as issued by the Social Security Administration requires an entity to have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1).

The National Technical Information Service has issued the Interim Final Rule for temporary certification permitting access to the Death Master File ("DMF"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, access to the DMF is restricted to only those entities that have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. §

1110.102(a)(1). As many Experian services contain information from the DMF, Experian would like to remind you of your continued obligation to restrict your use of deceased flags or other indicia within the Experian services to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with your applicable Fair Credit Reporting Act (15 U.S.C. §1681 et seq.) or Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) use. Your continued use of Experian services affirms your commitment to comply with these terms and all applicable laws.

You acknowledge you will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Experian services.

10) Scott-Roberts and Associates, LLC's Obligations.

A. Compliance with Applicable Laws. Scott-Roberts and Associates, LLC agrees to comply with all laws applicable to the making of Reports. Among other things, Scott-Roberts and Associates, LLC will: (a) follow reasonable procedures to assure maximum possible accuracy of the information reported, (b) disclose to Consumer, upon request, the information in the Consumer's file, and (c) reinvestigate any information disputed by the Consumer at no charge to the Client and take any necessary action to rectify a report that has been determined to have incorrect or unverifiable information.

B. Scope of Information Provided. Scott-Roberts and Associates, LLC shall seek out and deliver information consistent with the service descriptions set forth on its website at https://www.scottrobertsassociates.com/ at the time of the relevant search. Client understands that it must review and consider the scope of a search before placing an order with Scott-Roberts and Associates, LLC. Client also understands that it will not receive information from Scott-Roberts and Associates, LLC that falls outside of a requested search, and that it will not receive information that Scott-Roberts and Associates, LLC determines—in its sole discretion—to be unreportable under applicable law.

C. Administrative Role As To Adverse Action. If Client elects to have Scott-Roberts and Associates, LLC send out pre- and/or post-adverse action letters for it, Client understands that it must notify Scott-Roberts and Associates, LLC each time it wishes for a letter to go out. Scott-Roberts and Associates, LLC will not send out any adverse action letters unless expressly instructed to do so. Client accepts full responsibility for the content of any adverse action letters sent by Scott-Roberts and Associates, LLC, and understands that it must notify Scott-Roberts and Associates, LLC if it wishes to use a particular template or if it wishes to modify the template made available through Scott-Roberts and Associates, LLC. Client agrees that Scott-Roberts and Associates, LLC plays no role in deciding whether an individual should incur adverse action based upon a background screening report. Client accepts full responsibility for any and all substantive decision-making based upon the background screening reports it receives from Scott-Roberts and Associates, LLC. Both parties agree that Scott-Roberts and Associates, LLC's role as to the adverse action process is strictly administrative. Client shall indemnify, defend, and hold harmless Scott-Roberts and Associates, LLC, its affiliates, and subsidiaries and their respective officers, directors, employees, agents, and insurers from and against any and all damages, penalties, losses, liabilities, judgments, settlements, awards, costs, and expenses (including reasonable attorneys' fees and expenses) arising out of or in connection with any claims, assertions, demands, causes of action, suits, proceedings or other actions, whether at law or in equity ("Claims") related to the functions carried out by Scott-Roberts and Associates, LLC that are described in this section.

11) **Decision-making.** Client understands and agrees that Scott-Roberts and Associates, LLC does not make the decision to deny employment, deny tenancy, or take any other adverse action based on any reports prepared by Scott-Roberts and Associates, LLC. This responsibility falls solely with the Client. Client accepts full responsibility for any decision or adverse action made in part or whole on a Report provided by Scott-Roberts and Associates, LLC.

12) **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.

13) **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.

14) **Warranties and Indemnification.** Scott-Roberts and Associates, LLC assembles information from a variety of sources, including databases maintained by consumer reporting agencies containing information from public records, other information repositories, and third-party researchers. 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. Nevertheless, Scott-Roberts and Associates, LLC has in place procedures designed to ensure the maximum possible accuracy of the information reported and also 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; SCOTT-ROBERTS AND ASSOCIATES, LLC, EXPRESSLY DISCLAIMS ANY AND ALL SUCH REPRESENTATIONS AND WARRANTIES.

Client agrees to indemnify 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, and/or (iii) Client's negligence, misconduct, recklessness, errors or omissions.

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.

Client also understands that sample forms or documents made available by Scott-Roberts and Associates, LLC, to Client, including, but not limited to, sample disclosure notices, written authorizations, and adverse action notices are offered solely as a courtesy and should not be construed as legal advice. Laws governing the content of such documents frequently change. Accordingly, Client shall consult with counsel to make sure that it is using appropriate documents that comply with any and all applicable federal, state, and local laws. Use of Scott-Roberts and Associates, LLC's sample documents or processes—including any process designed to obtain the consumer's consent to the background check—is entirely optional. Therefore, if Client chooses to use Scott-Roberts and Associates, LLC's sample documents or processes in part or whole, Client agrees that such documents/processes should be considered its own (not that of Scott-Roberts and Associates, LLC), and that Client has consulted with its own legal counsel to the extent necessary regarding the use of such documents/processes. Client shall indemnify, defend, and hold harmless Scott-Roberts and Associates, LLC, its vendors and service providers, affiliates, and subsidiaries and their respective officers, directors, and employees from and against any and all damages, penalties, losses, liabilities, judgments, settlements, awards, costs, and expenses (including reasonable attorneys' fees and expenses) arising out of or in connection with any claims, assertions, demands, causes of action, suits, proceedings or other actions, whether at law or in equity ("Claims"), related to Client's use of sample forms, sample documents, or processes made available by Scott-Roberts and Associates, LLC.

15) **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. 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.

16) **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.

17) **Receipt of Federal Notices**. Client hereby acknowledges that it has received a copy of the federal notices entitled "A Summary of Your Rights Under the Fair Credit Reporting Act" and "Notice to Users of Consumer Reports."

18) **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 other 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, LLC's sole obligation will be to use its reasonable efforts to reconstruct any records maintained by Scott-Roberts and Associates, LLC and to amend any reports prepared by it with may have been affected by such event, at its own expense.

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

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

21) **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.

22) **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.

23) **Audits.** Client acknowledges that Scott-Roberts and Associates, LLC and certain third-party vendors, such as departments of motor vehicles and credit bureaus, are required to conduct periodic audit of Client's compliance with s.3 of this agreement. Client shall provide Scott-Roberts and Associates with reasonable documentation required for such audits at the Client's sole descretion. Scott-Roberts and Associates, LLC will provide reasonable notice prior to conducting any audit provided that Scott-Roberts and Associates, LLC has received reasonable notice from any third-party vendor involved in the audit process. Any violations discovered as a result of such audit may be cause for immediate action by Scott-Roberts and Associates, LLC, including, but not limited to, immediate termination of this Agreement.

24) **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.

25) **Successors and Assigns.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and assigns, provided, however, Client shall not assign or otherwise transfer this Agreement or any interest herein without the prior written consent of Scott-Roberts and Associates, LLC.

26) **No Third-Party Beneficiaries.** Except as specifically provided for herein, this Agreement shall not confer any rights or remedies upon any person other than the parties hereto and their respective successors and permitted assigns.

27) **Survival.** The following provisions shall survive termination of this Agreement: 3(A)(iv), 3(A)(v), 3(B)(iii), 5, 6, 7, 8(B)(v), 9, 11, 12, 14, 15, 18, 19, 20, 21, 22, and 2

28) **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, LLC:

Robert Buchholz or Sydnie Keeter Date:

Client Information:

Organization Name: Telephone: Fax:

Primary Contact Name: Title: Telephone: E-mail:

Street Address: City, State: ZIP:

NATURE OF BUSINESS:

The following persons are authorized to access the account:

Contact Name: Contact Email:

Contact Name: Contact Email:

APPLICATION TO BECOME A 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:_____ 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: _____

City: _____ State: _____ Zip: _____ How Long?_____(yrs)_____(mos)

Phone Number:_____ 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 <u>sole owner</u> or <u>partnership</u>, 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: _____

Residential Street Address: _____

City: _____ State: _____ Zip: _____

AFFILIATED OR PARENT COMPANY:

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

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

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.

_____

_____

_____

_____

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:

_____ _____
Typed or Printed Name of Owner or Officer: Title:

_____ _____
Authorized Signature: Date:

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. You can review a copy of the FCRA at http://www.ftc.gov/os/statutes/fcrajump.htm. We suggest that you and your employees become familiar with the following sections in particular:

- § **604. Permissible Purposes of Reports**
- § **607. Compliance Procedures**
- § **610. Conditions and Form of Disclosure to Consumers**
- § **611. Procedure in Case of Disputed Accuracy**
- § **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**
- § **620. Unauthorized Disclosures by Officers or Employees**
- § **621. Administrative Enforcement**
- § **623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies**

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.

Experian strongly endorses 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 statues *and the statues and regulation 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.

Para información en español, visite www.consumerfinance.gov/learnmore o escribe a la Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

A Summary of Your Rights Under the Fair Credit Reporting Act

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under FCRA. **For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.**

- **You must be told if information in your file has been used against you.** Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment – or to take another adverse action against you – must tell you, and must give you the name, address, and phone number of the agency that provided the information.

- **You have the right to know what is in your file.** You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free file disclosure if:

    - a person has taken adverse action against you because of information in your credit report;
    - you are the victim of identity theft and place a fraud alert in your file;
    - your file contains inaccurate information as a result of fraud;
    - you are on public assistance;
    - you are unemployed but expect to apply for employment within 60 days.

    In addition, all consumers are entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. See www.consumerfinance.gov/learnmore for additional information.

- **You have the right to ask for a credit score.** Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

- **You have the right to dispute incomplete or inaccurate information.** If you identify information in your file that is incomplete or inaccurate, and report it to the consumer

reporting agency, the agency must investigate unless your dispute is frivolous. See www.consumerfinance.gov/learnmore for an explanation of dispute procedures.

- **Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.** Inaccurate, incomplete, or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

- **Consumer reporting agencies may not report outdated negative information.** In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

- **Access to your file is limited.** A consumer reporting agency may provide information about you only to people with a valid need – usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

- **You must give your consent for reports to be provided to employers.** A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. For more information, go to www.consumerfinance.gov/learnmore.

- **You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.** Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address form the lists these offers are based on. You may opt out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).

- The following FCRA right applies with respect to nationwide consumer reporting agencies**:**

  CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

  You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

  As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is

placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

- **You may seek damages from violators.** If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

- **Identity theft victims and active duty military personnel have additional rights.** For more information, visit www.consumerfinance.gov/learnmore.

States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General. For information about your federal rights, contact:

TYPE OF BUSINESS:	CONTACT:
1.a. Banks, savings associations, and credit unions with total assets of over $10 billion and their affiliates b. Such affiliates that are not banks, savings associations, or credit unions also should list, in addition to the CFPB:	a. Consumer Financial Protection Bureau 1700 G Street, N.W. Washington, DC 20552 b. Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. Washington, DC 20580 (877) 382-4357
2. To the extent not included in item 1 above: a. National banks, federal savings associations, and federal branches and federal agencies of foreign banks b. State member banks, branches and agencies of foreign banks (other than federal branches, federal agencies, and Insured State Branches of Foreign Banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act. c. Nonmember Insured Banks, Insured State Branches of Foreign Banks, and insured state savings associations d. Federal Credit Unions	a. Office of the Comptroller of the Currency Customer Assistance Group 1301 McKinney Street, Suite 3450 Houston, TX 77010-9050 b. Federal Reserve Consumer Help Center P.O. Box 1200 Minneapolis, MN 55480 c. FDIC Consumer Response Center 1100 Walnut Street, Box #11 Kansas City, MO 64106 d. National Credit Union Administration Office of Consumer Financial Protection (OCFP) Division of Consumer Compliance Policy and Outreach 1775 Duke Street Alexandria, VA 22314
3. Air carriers	Asst. General Counsel for Aviation Enforcement & Proceedings Aviation Consumer Protection Division Department of Transportation 1200 New Jersey Avenue, S.E. Washington, DC 20590
4. Creditors Subject to the Surface Transportation Board	Office of Proceedings, Surface Transportation Board Department of Transportation 395 E Street, S.W. Washington, DC 20423
5. Creditors Subject to the Packers and Stockyards Act, 1921	Nearest Packers and Stockyards Administration area supervisor
6. Small Business Investment Companies	Associate Deputy Administrator for Capital Access United States Small Business Administration 409 Third Street, S.W., Suite 8200 Washington, DC 20416
7. Brokers and Dealers	Securities and Exchange Commission 100 F Street, N.E. Washington, DC 20549
8. Federal Land Banks, Federal Land Bank Associations, Federal Intermediate Credit Banks, and Production Credit Associations	Farm Credit Administration 1501 Farm Credit Drive McLean, VA 22102-5090
9. Retailers, Finance Companies, and All Other Creditors Not Listed Above	Federal Trade Commission Consumer Response Center 600 Pennsylvania Avenue, N.W. Washington, DC 20580 (877) 382-4357

NOTICES TO FURNISHERS OF INFORMATION: OBLIGATIONS OF FURNISHERS UNDER THE FCRA

The federal Fair Credit Reporting Act ("FCRA"), as amended, imposes responsibilities on all persons who furnish information to consumer reporting agencies ("CRAs"). These responsibilities are found in Section 623 of the FCRA. State law may impose additional requirements. All furnishers of information to CRAs should become familiar with the law and may want to consult with their counsel to ensure that they are in compliance. The FCRA, 15 U.S.C. §§ 1681-1681u, is set forth in full at the Federal Trade Commission's Internet web site *(http://www.ftc.gov)*. Section 623 imposes the following duties:

General Prohibition on Reporting Inaccurate Information:

The FCRA prohibits information furnishers from providing information to a consumer reporting agency ("CRA") that they know (or consciously avoid knowing) is inaccurate. However, the furnisher is not subject to this general prohibition if it clearly and conspicuously specifies an address to which consumers may write to notify the furnisher that certain information is inaccurate. *Sections 623(a)(1)(A) and (a)(1)(C)*

Duty to Correct and Update Information:

If at any time a person who regularly and in the ordinary course of business furnishes information to one or more CRAs determines that the information provided is not complete or accurate, the furnisher must provide complete and accurate information to the CRA. In addition, the furnisher must notify all CRAs that received the information of any corrections, and must thereafter report only the complete and accurate information. *Section 623(a)(2)*

Duties After Notice of Dispute from Consumer:

If a consumer notifies a furnisher, at an address specified by the furnisher for such notices, that specific information is inaccurate, and the information is in fact inaccurate, the furnisher must thereafter report the correct information to CRAs. *Section 623(a)(1)(B)*

If a consumer notifies a furnisher that the consumer disputes the completeness or accuracy of any information reported by the furnisher, the furnisher may not subsequently report that information to a CRA without providing notice of the dispute. *Section 623(a)(3)*

Duties After Notice of Dispute from Consumer Reporting Agency:

If a CRA notifies a furnisher that a consumer disputes the completeness or accuracy of information provided by the furnisher, the furnisher has a duty to follow certain procedures. The furnisher must:

- Conduct an investigation and review all relevant information provided by the CRA, including information given to the CRA by the consumer. *Sections 623(b)(1)(A) and (b)(1)(B)*
- Report the results to the CRA, and, if the investigation establishes that the information was, in fact, incomplete or inaccurate, report the results to all CRAs to which the furnisher provided the information that compile and maintain files on a nationwide basis. *Sections 623(b)(1)(C) and (b)(1)(D)*
- Complete the above within 30 days from the date the CRA receives the dispute (or 45 days, if the consumer later provides relevant additional information to the CRA). *Section 623(b)(2)*

Duty to Report Voluntary Closing of Credit Accounts:

If a consumer voluntarily closes a credit account, any person who regularly and in the ordinary course of business furnishes information to one or more CRAs must report this fact when it provides information to CRAs for the time period in which the account was closed. *Section 623(a)(4)*

Duty to Report Dates of Delinquencies:

If a furnisher reports information concerning a delinquent account placed for collection, charged to profit or loss, or subject to any similar action, the furnisher must, within 90 days after reporting the information, provide the CRA with the month and the year of the commencement of the delinquency that immediately preceded the action, so that the agency will know how long to keep the information in the consumer's file. *Section 623(a)(5)*

NOTICE TO USERS OF CONSUMER REPORTS: OBLIGATIONS OF USERS UNDER THE FCRA

The federal Fair Credit Reporting Act (FCRA) requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. This first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that areused for certain purposes, and the legal consequences of violations. The FCRA, 15 U.S.C. §§ 1681-1681u, is set forth in full at the Federal Trade Commission's Internet web site *(http://www.ftc.gov)*.

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 of the FCRA contains a list of the permissible purposes under the law. These are:

- As ordered by a court or a federal grand jury subpoena. *Section 604(a)(1)*
- As instructed by the consumer in writing. *Section 604(a)(2)*
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. *Section 604(a)(3)(A)*
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. *Sections 604(a)(3)(B) and 604(b)*
- For the underwriting of insurance as a result of an application from a consumer. *Section 604(a)(3)(C)*
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. *Section 604(a)(3)(F)(i)*
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. *Section 604(a)(3)(F)(ii)*
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. *Section 604(a)(3)(D)*
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or repayment risks associated with an existing credit obligation. *Section 604(a)(3)(E)*
- For use by state and local officials in connection with the determination of child support payments, or modifications and enforcement thereof. *Sections 604(a)(4) and 604(a)(5)*

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making unsolicited offers of credit or insurance. The particular obligations of users of this "prescreened" information are described in Section V below.

B. Users Must Provide Certifications

Section 604(f) of the FCRA prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA (by a general or specific certification, as appropriate) the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term "adverse action" is defined very broadly by Section 603 of the FCRA. "Adverse actions" include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact -- such as unfavorably changing credit or contract terms or conditions, denying or canceling credit or insurance, offering credit on less favorable terms than requested, or denying employment or promotion.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action that is based at least in part on information contained in a consumer report, the user is required by Section 615(a) of the FCRA to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer requests the report within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained From Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) of the FCRA requires that the user clearly and accurately disclose to the consumer his or her right to obtain disclosure of the nature of the information that was relied upon by making a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notification must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. (Information that is obtained directly from an affiliated entity relating solely to its transactions or experiences with the consumer, and information from a consumer report obtained from an affiliate are not covered by Section 615(b)(2).)

II. OBLIGATIONS OF USERS WHEN CONSUMER REPORTS ARE OBTAINED FOR EMPLOYMENT PURPOSES

If information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain prior written authorization from the consumer.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.
- Before taking an adverse action, provide a copy of the report to the consumer as well as the summary of the consumer's rights. (The user should receive this summary from the CRA, because Section 604(b)(1)(B) of the FCRA requires CRAs to provide a copy of the summary with each consumer report obtained for employment purposes.)

III. OBLIGATIONS OF USERS OF INVESTIGATIVE CONSUMER REPORTS

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews. Consumers who are the subjects of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 of the FCRA requires the following:

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer not later than three days after the date on which the report was first requested. The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and must include the summary of consumer rights required by Section 609 of the FCRA. (The user should be able to obtain a copy of the notice of consumer rights from the CRA that provided the consumer report.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure described below.
- Upon the written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation that was requested. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

IV. OBLIGATIONS OF USERS OF CONSUMER REPORTS CONTAINING MEDICAL INFORMATION

Section 604(g) of the FCRA prohibits consumer reporting agencies from providing consumer reports that contain medical information for employment purposes, or in connection with credit or insurance transactions, without the specific prior consent of the consumer who is the subject of the report. In the case of medical information being sought for employment purposes, the consumer must explicitly consentto the release of the medical information in addition to authorizing the obtaining of a consumer report generally.

V. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. *Sections 603(l), 604(c), 604(e), and 615(d)* This practice is known as "prescreening" and typically involves obtaining a list of consumers from a CRA who meet certain preestablished criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in the consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or anyapplicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.
- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. This statement must include the address and toll-free telephone number of the appropriate notification system.

VI. OBLIGATIONS OF RESELLERS

Section 607(e) of the FCRA requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain: (1) the identity of all end-users; (2) certifications from all users of each purpose for which reports will be used; and (3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

VII. LIABILITY FOR VIOLATIONS OF THE FCRA

Failure to comply with the FCRA can result in state or federal enforcement actions, as well as private lawsuits. *Sections 616, 617, and 621* In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. *Section 619*

All users of consumer reports must comply with all applicable regulations. Information about applicable regulations currently in effect can be found at the Consumer Financial Protection Bureau's website, www.consumerfinance.gov/learnmore.

NOTICE TO USERS OF CONSUMER REPORTS: OBLIGATIONS OF USERS UNDER THE FCRA

The Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681-1681y, requires that this notice be provided to inform users of consumer reports of their legal obligations. State law may impose additional requirements. The text of the FCRA is set forth in full at the Consumer Financial Protection Bureau's (CFPB) website at www.consumerfinance.gov/learnmore. At the end of this document is a list of United States Code citations for the FCRA. Other information about user duties is also available at the Bureau's website. **Users must consult the relevant provisions of the FCRA for details about their obligations under the FCRA.**

The first section of this summary sets forth the responsibilities imposed by the FCRA on all users of consumer reports. The subsequent sections discuss the duties of users of reports that contain specific types of information, or that are used for certain purposes, and the legal consequences of violations. If you are a furnisher of information to a consumer reporting agency (CRA), you have additional obligations and will receive a separate notice from the CRA describing your duties as a furnisher.

I. Obligations of All Users of Consumer Reports

A. Users Must Have a Permissible Purpose

Congress has limited the use of consumer reports to protect consumers' privacy. All users must have a permissible purpose under the FCRA to obtain a consumer report. Section 604 contains a list of the permissible purposes under the law. These are:

- As ordered by a court or federal grand jury subpoena. Section 604(a)(1)
- As instructed by the consumer in writing. Section 604(a)(2)
- For the extension of credit as a result of an application from a consumer, or the review or collection of a consumer's account. Section 604(a)(3)(A)
- For employment purposes, including hiring and promotion decisions, where the consumer has given written permission. Section 604(a)(3)(B) and 604(b)
- For the underwriting of insurance as a result of an application from a consumer. Section 604(a)(3)(C)
- When there is a legitimate business need, in connection with a business transaction that is initiated by the consumer. Section 604(a)(3)(F)(i)
- To review a consumer's account to determine whether the consumer continues to meet the terms of the account. Section 604(a)(3)(F)(ii)
- To determine a consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status. Section 604(a)(3)(D)
- For use by a potential investor or servicer, or current insurer, in a valuation or assessment of the credit or prepayment risks associated with an existing credit obligation. Section 604(a)(3)(E)
- For use by state or local officials in connection with the determination of child support payments, or modifications and enforcement thereof. Sections 604(a)(4) and 604(a)(5).

In addition, creditors and insurers may obtain certain consumer report information for the purpose of making "prescreened" unsolicited offers of credit or insurance. Section 604(c). The particular obligations of users of "prescreened" information are described in Section VII below.

B. Users Must Provide Certifications

Section 604(f) prohibits any person from obtaining a consumer report from a consumer reporting agency (CRA) unless the person has certified to the CRA the permissible purpose(s) for which the report is being obtained and certifies that the report will not be used for any other purpose.

C. Users Must Notify Consumers When Adverse Actions Are Taken

The term "adverse action" is defined very broadly by Section 603. "Adverse actions" include all business, credit, and employment actions affecting consumers that can be considered to have a negative impact as defined by Section 603(k) of the FCRA – such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer.

1. Adverse Actions Based on Information Obtained From a CRA

If a user takes any type of adverse action as defined by the FCRA that is based at least in part on information contained in a consumer report, Section 615(a) requires the user to notify the consumer. The notification may be done in writing, orally, or by electronic means. It must include the following:

- The name, address, and telephone number of the CRA (including a toll-free telephone number, if it is a nationwide CRA) that provided the report.
- A statement that the CRA did not make the adverse decision and is not able to explain why the decision was made.
- A statement setting forth the consumer's right to obtain a free disclosure of the consumer's file from the CRA if the consumer makes a request within 60 days.
- A statement setting forth the consumer's right to dispute directly with the CRA the accuracy or completeness of any information provided by the CRA.

2. Adverse Actions Based on Information Obtained from Third Parties Who Are Not Consumer Reporting Agencies

If a person denies (or increases the charge for) credit for personal, family, or household purposes based either wholly or partly upon information from a person other than a CRA, and the information is the type of consumer information covered by the FCRA, Section 615(b)(1) requires that the user clearly and accurately disclose to the consumer his or her right to be told the nature of the information that was relied upon if the consumer makes a written request within 60 days of notification. The user must provide the disclosure within a reasonable period of time following the consumer's written request.

3. Adverse Actions Based on Information Obtained From Affiliates

If a person takes an adverse action involving insurance, employment, or a credit transaction initiated by the consumer, based on information of the type covered by the FCRA, and this information was obtained from an entity affiliated with the user of the information by common ownership or control, Section 615(b)(2) requires the user to notify the consumer of the adverse action. The notice must inform the consumer that he or she may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of receiving the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information not later than 30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure set forth in I.C.1 above.

D. Users Have Obligations When Fraud and Active Duty Military Alerts are in Files

When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers,

Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extendedfraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

Section 605(h) requires nationwide CRAs, as defined in Section 603(p), to notify users that request reports when the address for a consumer provided by the user in requesting the report is substantially different from the addresses in the consumer's file. When this occurs, users must comply with regulations specifying the procedures to be followed. Federal regulations are available at www.consumerfinance.gov/learnmore.

F. Users Have Obligations When Disposing of Records

Section 628 requires that all users of consumer report information have in place procedures to properly dispose of records containing this information. Federal regulations have been issued that cover disposal.

II. Creditors Must Make Additional Disclosures

If a person uses a consumer report in connection with an application for, or a grant, extension, or provision of, credit to a consumer on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person, based in whole or in part on a consumer report, the person must provide a risk-based pricing notice to the consumer in accordance with regulations prescribed by the Consumer Financial Protection Bureau.

Section 609(g) requires a disclosure by all persons that make or arrange loans secured by residential real property (one to four units) and that use credit scores. These persons must provide credit scores and other information about credit scores to applicants, including the disclosure set forth in Section 609(g)(1)(D) ("Notice to the Home Loan Applicant").

III. Obligations Of Users When Consumer Reports Are Obtained For Employment Purposes

A. Employment Other Than in the Trucking Industry

If information from a CRA is used for employment purposes, the user has specific duties, which are set forth in Section 604(b) of the FCRA. The user must:

- Make a clear and conspicuous written disclosure to the consumer before the report is obtained, in a document that consists solely of the disclosure, that a consumer report may be obtained.
- Obtain from the consumer prior written authorization. Authorization to access reports during the term of employment may be obtained at the time of employment.
- Certify to the CRA that the above steps have been followed, that the information being obtained will not be used in violation of any federal or state equal opportunity law or regulation, and that, if any adverse action is to be taken based on the consumer report, a copy of the report and a summary of the consumer's rights will be provided to the consumer.
- **Before** taking an adverse action, the user must provide a copy of the report to the consumer as well as the summary of the consumer's rights. (The user should receive this summary from the CRA.). A Section 615(a) adverse action notice should be sent after the adverse action is taken.

An adverse action notice also is required in employment situations if credit information (other than transactions and experience data) obtained from an affiliate is used to deny employment. Section 615(b)(2).

The procedures for investigative consumer reports and employee misconduct investigations are set forth below.

B. Employment in the Trucking Industry

Special rules apply for truck drivers where the only interaction between the consumer and the potential employer is by mail, telephone, or computer. In this case, the consumer may provide consent orally or electronically, and an adverse action may be made orally, in writing, or electronically. The consumer may obtain a copy of any report relied upon by the trucking company by contacting the company.

IV. Obligations When Investigative Consumer Reports Are Used

Investigative consumer reports are a special type of consumer report in which information about a consumer's character, general reputation, personal characteristics, and mode of living is obtained through personal interviews by an entity or person that is a consumer reporting agency. Consumers who are the subject of such reports are given special rights under the FCRA. If a user intends to obtain an investigative consumer report, Section 606 requires the following:

- The user must disclose to the consumer that an investigative consumer report may be obtained. This must be done in a written disclosure that is mailed, or otherwise delivered, to the consumer at some time before or not later than three days after the date on which the report was first requested.The disclosure must include a statement informing the consumer of his or her right to request additional disclosures of the nature and scope of the investigation as described below, and the summary of consumer rights required by Section 609 of the FCRA. (The summary of consumer rights will be provided by the CRA that conducts the investigation.)
- The user must certify to the CRA that the disclosures set forth above have been made and that the user will make the disclosure below.
- Upon written request of a consumer made within a reasonable period of time after the disclosures required above, the user must make a complete disclosure of the nature and scope of the investigation. This must be made in a written statement that is mailed, or otherwise delivered, to the consumer no later than five days after the date on which the request was received from the consumer or the report was first requested, whichever is later in time.

V. Special Procedures for Employee Investigations

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state or local laws and regulations or the rules of a self- regulatory organization, and compliance with written policies of the employer. These investigations arenot treated as consumer reports so long as the employer or its agent complies with the procedures setforth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. Obligations Of Users Of Medical Information

Section 604(g) limits the use of medical information obtained from consumer reporting agencies (other than payment information that appears in a coded form that does not identify the medical provider). If the information is to be used for an insurance transaction, the consumer must give consent to the user of the report or the information must be coded. If the report is to be used for employment purposes - or in connection with a credit transaction (except as provided in federal regulations) - the consumer must provide specific written consent and the medical information mustbe relevant. Any user who receives medical information shall not disclose the information to any otherperson (except where necessary to carry out the purpose for which the information was disclosed, or as permitted by statute, regulation, or order).

VII. Obligations Of Users Of "Prescreened" Lists

The FCRA permits creditors and insurers to obtain limited consumer report information for use in connection with unsolicited offers of credit or insurance under certain circumstances. Section 603(l), 604(c), 604(e), and 615(d). This practice is known as "prescreening" and typically involves obtaining from a CRA a list of consumers who meet certain pre-established criteria. If any person intends to use prescreened lists, that person must (1) before the offer is made, establish the criteria that will be relied upon to make the offer and to grant credit or insurance, and (2) maintain such criteria on file for

a three-year period beginning on the date on which the offer is made to each consumer. In addition, any user must provide with each written solicitation a clear and conspicuous statement that:

- Information contained in a consumer's CRA file was used in connection with the transaction.
- The consumer received the offer because he or she satisfied the criteria for credit worthiness or insurability used to screen for the offer.
- Credit or insurance may not be extended if, after the consumer responds, it is determined that the consumer does not meet the criteria used for screening or any applicable criteria bearing on credit worthiness or insurability, or the consumer does not furnish required collateral.
- The consumer may prohibit the use of information in his or her file in connection with future prescreened offers of credit or insurance by contacting the notification system established by the CRA that provided the report. This statement must include the address and the toll-free telephone number of the appropriate notification system.

In addition, once the CFPB has established the format, type size, and manner of the disclosure required by Section 615(d), with which users must comply. The relevant regulation is 12 CFR 1022.54.

VIII. Obligations of Resellers

A. Disclosure and Certification Requirements

Section 607(e) requires any person who obtains a consumer report for resale to take the following steps:

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain: 1) the identity of all end-users;

2) certifications from all users of each purposes for which reports will be used; and

3) certifications that reports will not be used for any purpose other than the purpose(s) specified to the reseller. Resellers must make reasonable efforts to verify this information before selling the report.

B. Reinvestigations by Resellers

Under Section 611(f), if a consumer disputes the accuracy or completeness of information in a report prepared by a reseller, the reseller must determine whether this is a result of an action or omission on its part and, if so, correct or delete the information. If not, the reseller must send the dispute to the source CRA for reinvestigation. When any CRA notifies the reseller of the results of an investigation, the reseller must immediately convey the information to the consumer.

C. Fraud Alerts and Resellers

Section 605A(f) requires resellers who receive fraud alerts or active duty alerts from another consumer reporting agency to include these in their reports.

IX. Liability For Violations Of The FCRA

Failure to comply with the FCRA can result in state government or federal government enforcement actions, as well as private lawsuits. Sections 616, 617, and 621. In addition, any person who knowingly and willfully obtains a consumer report under false pretenses may face criminal prosecution. Section 619.

The CFPB's website, www.consumerfinance.gov/learnmore, has more information about the FCRA, including publications for businesses and the full text of the FCRA.

Citations for the FCRA sections in the U.S. Code, 15 U.S.C.§ 1681 et seq.:

Section 602 15 U.S.C. 1681
Section 603 15 U.S.C. 1681a
Section 604 15 U.S.C. 1681b
Section 605 15 U.S.C. 1681c
Section 605A 15 U.S.C. 1681cA
Section 605B 15 U.S.C. 1681cB
Section 606 15 U.S.C. 1681d
Section 607 15 U.S.C. 1681e
Section 608 15 U.S.C. 1681f
Section 609 15 U.S.C. 1681g
Section 610 15 U.S.C. 1681h
Section 611 15 U.S.C. 1681i
Section 612 15 U.S.C. 1681j
Section 613 15 U.S.C. 1681k
Section 614 15 U.S.C. 1681*l*
Section 615 15 U.S.C. 1681m
Section 616 15 U.S.C. 1681n
Section 617 15 U.S.C. 1681o
Section 618 15 U.S.C. 1681p
Section 619 15 U.S.C. 1681q
Section 620 15 U.S.C. 1681r
Section 621 15 U.S.C. 1681s
Section 622 15 U.S.C. 1681s-1
Section 623 15 U.S.C. 1681s-2
Section 624 15 U.S.C. 1681t
Section 625 15 U.S.C. 1681u
Section 626 15 U.S.C. 1681v
Section 627 15 U.S.C. 1681w
Section 628 15 U.S.C. 1681x
Section 629 15 U.S.C. 1681y

Access Security Requirements for FCRA and GLB 5A Data

The following information security controls are required to reduce unauthorized access to consumer information. It is your (company provided access to Experian systems or data, referred to as the "Company") responsibility to implement these controls. If you do not understand these requirements or need assistance, it is your responsibility to get an outside service provider to assist you. Experian reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security.

In accessing Experian's services, Company agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store Experian data:

1. Implement Strong Access Control Measures

1.1 All credentials such as Subscriber Code number, Subscriber Code passwords, User names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Experian will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Experian's systems, ensure that the access must be preceded by authenticating users to the application and/or system (e.g. application based authentication, Active Directory, etc.) utilized for accessing Experian data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access Experian data/systems, is replaced or no longer in use, the passwords should be changed immediately.

1.4 Create a 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.

1.5 User IDs and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.

1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.

1.7 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 eight (8) alphabetic and numeric characters for standard user accounts
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

1.8 Passwords (e.g. subscriber code passwords, user password) must 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
- Any suspicion of password being

1.9 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure that strong encryption algorithm are utilized (e.g. AES 256 or above).

1.10 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

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

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 the membership application.

Access Security Requirements for FCRA and GLB 5A Data

1. Implement Strong Access Control Measures

1.13 Company must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Experian data.

1.14 Ensure that Company employees do not access their 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.

1.15 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.

1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.

1.17 Implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.18 Implement physical security controls to prevent unauthorized entry to Company's facility and access to systems used to obtain credit information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

2. Maintain a Vulnerability Management Program

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and 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 anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

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 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document 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 electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

3. Protect Data

3.5	Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.
3.6	When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass-code.
3.7	Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.
3.8	Only open email attachments and links from trusted sources and after verifying legitimacy.
3.9	When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.
3.10	When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

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 Safeguards Rule.
4.2	Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.
4.3	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. If you believe Experian data may have been compromised, immediately notify Experian within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).
4.4	The FACTA Disposal Rules requires that Company 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.
4.5	Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.
4.6	When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Company responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. Approved certifications in lieu of EI3PA can be found in the Glossary section.

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. Build and Maintain a Secure Network

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	Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.
5.6	For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.
5.7	When using service providers (e.g. software providers) to access Experian systems, access to third party tools/services must require multi-factor authentication.

6. Regularly Monitor and Test Networks

6.1	Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)
6.2	Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Experian data; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.
6.3	Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Experian 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.

7. Mobile and Cloud Technology

7.1	Storing Experian data on mobile devices is prohibited. Any exceptions must be obtained from Experian in writing; additional security requirements will apply.
7.2	Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.
7.3	Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.
7.4	Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.
7.5	Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non-secured applications on the mobile device.

7. Mobile and Cloud Technology

7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Experian data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

7.7 When using cloud providers to access, transmit, store, or process Experian data ensure that:

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Experian:
  - ISO 27001
  - PCI DSS
  - EI3PA
  - SSAE 16 – SOC 2 or SOC3
  - FISMA
  - CAI / CCM assessment

8. General

8.1 Experian may from time to time audit the security mechanisms Company maintains to safeguard access to Experian information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices

8.2 In cases where the Company is accessing Experian information and systems via third party software, the Company agrees to make available to Experian upon request, audit trail information and management reports generated by the vendor software, regarding Company individual Authorized Users.

8.3 Company shall be responsible for and ensure that third party software, which accesses Experian information systems, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.

8.4 Company shall conduct software development (for software which accesses Experian information systems; this applies to both in-house or outsourced software development) based on the following requirements:

8.4.1 Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.

8.4.2 Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

8.4.3 Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

8.5 Reasonable access to audit trail reports of systems utilized to access Experian systems shall be made available to Experian upon request, for example during breach investigation or while performing audits

8.6 Data requests from Company to Experian must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

8.7 Company shall report actual security violations or incidents that impact Experian to Experian within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Experian of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 800-295-4305, Email notification will be sent to regulatorycompliance@experian.com.

8. General

8.8	Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to Experian services, systems or data, and (d) will abide by the provisions of these requirements when accessing Experian data.
8.9	Company understands that its use of Experian networking and computing resources may be monitored and audited by Experian, without further notice.
8.10	Company acknowledges and agrees that it is responsible for all activities of its employees/Authorized users, and for assuring that mechanisms to access Experian services or data are secure and in compliance with its membership agreement.
8.11	When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by Experian.

Record Retention: The Federal Equal Credit Opportunity 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 $3,500 per violation."

Access Security Requirements for FCRA and GLB 5A Data

Internet Delivery Security Requirements

In addition to the above, following requirements apply where Company and their employees or an authorized agent/s acting on behalf of the Company are provided access to Experian provided services via Internet ("Internet Access").

General Requirements

1. The Company shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Experian on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Experian provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.
2. The Company's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Experian product based upon the legitimate business needs of each employee. Experian shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.
3. Unless automated means become available, the Company shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by Experian. Those employees approved by the Head Security Designate or Security Designate for Internet access ("Authorized Users") will be individually assigned unique access identification accounts ("User ID") and passwords/passphrases (this also applies to the unique Server-to-Server access IDs and passwords/passphrases). Experian's approval of requests for (Internet) access may be granted or withheld in its sole discretion. Experian may add to or change its requirements for granting (Internet) access to the services at any time (including, without limitation, the imposition of fees relating to (Internet) access upon reasonable notice to Company), and reserves the right to change passwords/passphrases and to revoke any authorizations previously granted. Note: Partially completed forms and verbal requests will not be accepted.
4. An officer of the Company agrees to notify Experian in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with Experian on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with Experian on information and product access, in accordance with these Experian Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to Experian's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Experian immediately.
2. As a Client to Experian's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.

Access Security Requirements for FCRA and GLB 5A Data

Roles and Responsibilities

3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to Experian product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with Experian's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding Experian representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

1. Must be an employee and duly appointed representative of Company, identified as an approval point for Company's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Company's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).
3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.
4. Is responsible for ensuring that Company's Authorized Users are authorized to access Experian products and services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Company.
6. Must immediately report any suspicious or questionable activity to Experian regarding access to Experian's products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Experian.
8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
9. Shall be available to interact with Experian when needed on any system or user related matters.

Access Security Requirements for FCRA and GLB 5A Data

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.
Subscriber Code	Your seven digit Experian account number.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA℠ requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA℠ also establishes quarterly scans of networks for vulnerabilities.

Access Security Requirements for FCRA and GLB 5A Data

Glossary

ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard). The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report , just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

My Signature confirms that I have read, understood, and will comply with the Access Security Requirements for FCRA and GLB 5A Data.

Signature:

Printed Name:

Important Notice – Death Master File

Access to the Death Master File as issued by the Social Security Administration requires an entity to have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1).

The National Technical Information Service has issued the Interim Final Rule for temporary certification permitting access to the Death Master File ("DMF"). Pursuant to Section 203 of the Bipartisan Budget Act of 2013 and 15 C.F.R. § 1110.102, access to the DMF is restricted to only those entities that have a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule regulation, or fiduciary duty, as such business purposes are interpreted under 15 C.F.R. § 1110.102(a)(1). As many Experian services contain information from the DMF, Experian would like to remind you of your continued obligation to restrict your use of deceased flags or other indicia within the Experian services to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with your applicable Fair Credit Reporting Act (15 U.S.C. §1681 *et seq*.) or Gramm-Leach-Bliley Act (15 U.S.C. § 6801 *et seq*.) use. Your continued use of Experian services affirms your commitment to comply with these terms and all applicable laws.

You acknowledge you will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within the Experian services.

Experian

Access Security Requirements

For GLB VB and White Page Data

We must work together to protect the privacy of consumers. The following measures are designed to reduce unauthorized access of consumer information. In accessing consumer information products, you agree to follow these measures.

1. You must protect your account number and password so that only key personnel employed by your company know this sensitive information. Unauthorized persons should never have knowledge of your password. Do not post this information in any manner within your facility. If a person who knows the password leaves your company or no longer needs to have it due to a change in duties, the password should be changed immediately.

2. System access software, whether developed by your company or purchased from a third party vendor, must have your account number and password "hidden" or embedded and be known only by supervisory personnel. Assign each user of your system access software a unique logon password. If such system access software is replaced by different access software and therefore no longer in use or, alternatively, the hardware upon which such system access software resides is no longer being used or is being disposed of, your password should be changed immediately.

3. Do not discuss your account number and password by telephone with any unknown caller, even if the caller claims to be an employee of your credit provider.

4. Restrict the ability to obtain consumer information products-to a few key personnel.

5. Place all terminal devices used to obtain consumer information products in a secure location within your facility. You should secure these devices so that unauthorized persons cannot easily access them.

6. After normal business hours, be sure to turn off and lock all devices or systems used to obtain consumer information products.

7. Secure hard copies and electronic files of consumer information products within your facility so that unauthorized persons cannot easily access them.

8. Shred or destroy all hard copy consumer information products when no longer needed.

9. Erase and overwrite or scramble electronic files containing consumer information when no longer needed and when applicable regulation(s) permit destruction.

10. Make all employees aware that your company can access consumer information products only for the GLB Exception Appropriate use/Appropriate industry listed on GLB Matrix section of your membership application. You or your employees may not access their own information. Nor should you or your employees' access information of a family member or friend unless it is in connection with an appropriate GLB transaction.

I agree to implement and adhere to the above controls.

Date	Signature
Company Name	Print Name / Title

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. You can review a copy of the FCRA at http://www.ftc.gov/os/statutes/fcrajump.htm. We suggest that you and your employees become familiar with the following sections in particular:

- § **604. Permissible Purposes of Reports**
- § **607. Compliance Procedures**
- § **610. Conditions and Form of Disclosure to Consumers**
- § **611. Procedure in Case of Disputed Accuracy**
- § **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**
- § **620. Unauthorized Disclosures by Officers or Employees**
- § **621. Administrative Enforcement**
- § **623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies**

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.

Experian strongly endorses 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 statues *and the statues and regulation 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