DATA FACTS℠
Information You Trust

Data Facts Gives Back Sign-Up

GIVES. BACK.

Data Facts will donate 10% of the first month of billing to the charity of your choice.

*Charity must have a 501(c)(3) exemption to be eligible. If you do not have a specific charity in mind, we have provided a list of 6 worthwhile charities from which you can choose.

Date: _____

Name of Company: _____

Address: _____

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

Name of Charity: _____

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

ARDC ardreamcenter.tv

Big Brothers Big Sisters of Middle Tennessee

Habitat for Humanity of Greater Memphis of Greater Nashville

houston foodbank

Ronald McDonald House Charities Memphis Tampa Bay
Keeping families close

Youth VILLAGES

DATA FACTS℠
Information You Trust

Data Facts Gives Back Sign-Up

ARDC
ardreamcenter.tv

The Arkansas Dream Center strives to help solve moral decay, crime, drugs, gangs, homelessness and poverty epidemics that exist throughout Arkansas. The vision of the Arkansas Dream Center is to see thousands of hurting people come to know a new life through the efforts of their staff, volunteers, and recently rehabilitated individuals whose lives have been dramatically changed.

Big Brothers Big Sisters
of Middle Tennessee

For more than 100 years, Big Brothers Big Sisters has operated under the belief that inherent in every child is the ability to succeed and thrive in life. As the nation's largest donor and volunteer supported mentoring network, Big Brothers Big Sisters makes meaningful, monitored matches between adult volunteers ("Bigs") and children ("Littles"), ages 6 through 18, in communities across the country. They develop positive relationships that have a direct and lasting effect on the lives of young people.

Habitat for Humanity®
of Greater Memphis
of Greater Nashville

Habitat works in partnership with families in need of adequate shelter to build decent, affordable homes. The homes are then sold to Habitat's partner families, at no profit and with no interest charged. Partner families invest hundreds of hours of their own labor — sweat equity — into building their homes and the homes of others. Their mortgage payments go into a revolving "Fund for Humanity" that is used to build more homes.

houston foodbank

The Houston Food Bank is America's largest food bank in distribution to its network of 600 hunger relief charities in 18 southeast Texas counties. Named top charity in Texas by Charity Navigator for financial performance and accountability, the Houston Food Bank provides 83 million nutritious meals to food pantries, soup kitchens, senior centers and other agencies, feeding 800,000 people each year.

Ronald McDonald House Charities®
Memphis Tampa Bay
Keeping families close®

Ronald McDonald House Charities of Memphis, at no charge to guests, provides supportive services and "keeps families close"® while children are receiving treatment for cancer and other catastrophic childhood illnesses at St. Jude Children's Research Hospital. Ronald McDonald House Tampa Bay is comprised of four Houses, three in St. Petersburg and one in Tampa, offering 80 bedrooms with private baths. Together, the Houses became a "home-away-from-home" and serve 2,000 pediatric families annually. The supportive environment at each of the Houses, offered through dedicated volunteers, staff and other residents, provides comfort and care to those who supply the love, understanding, nurturing and emotional support essential for their child's recovery from illness or injury.

Youth
VILLAGES

Youth Villages is a nationally recognized nonprofit that works with the troubled children often forgotten by society or deemed beyond hope. Their work is successful because they do whatever it takes to save a child by strengthening, restoring, empowering their families. Year after year, the data prove the power of the Youth Villages approach, which is called Evidentiary Family Restoration®. Even two years after kids have completed their program, more than 80 percent are still living successfully with their families in their communities, reporting no trouble with the law. The key to radically improved, lasting outcomes for our most vulnerable children is restoring families, restoring accountability, restoring trust.

Membership Application Checklist

(must be completed prior to account activation)

Date: _____

Company Name: _____

Physical Address (no P.O. Box numbers please): _____

City/State/Zip: _____ How long? ____ years ____ months

What type of business location are you in? (please check one): ☐ Commercial ☐ Residential
Do you own or lease the building in which you are located (please check one): ☐ Own ☐ Lease

Company Phone: _____ Contact Phone: _____ Fax: _____

Email:_____ Federal Tax ID: _____

Website Address: _____

Previous Address (*If less than 5 years at current*): _____

City/State/Zip: _____How long? ____ years ____ months

Type of ownership (indicate one): ☐ Partnership ☐ Sole Owner ☐ Nonprofit ☐ Corporation

If sole owner or partnership, please complete this section:

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

Principal Name: _____ Title/Position: _____

Phone number: _____ Social Security Number: _____ Year of Birth: _____

Residential Street Address: _____

City/State/Zip: _____

Affiliated or Parent Company Name:_____

Contact Name: _____ Title:_____

Street Address: _____ Phone: _____

City/State/Zip: _____

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

Note in which states you do business:_____

What is the nature of your business? _____

Do you consider your business to be primarily ☐ Local ☐ Regional ☐ National

How long has your company been in business? _____ years _____ months

For what purpose will you use Data Facts services?

☐ Mortgage ☐ Employee Screening ☐ Tenant Screening ☐ Other: _____

What do you believe your permissible purpose is: _____

If you are using Data Facts for Consumer Reports, will you be pulling credit? ☐ Yes ☐ No

If you will be pulling credit reports, # of estimated credit reports you will access monthly: _____

How will you access consumer reports? ☐ Personal Computer ☐ Phone/Fax ☐ Other _____

I have received and understand my responsibilities under the Fair Credit Reporting Act. ☐ Yes ☐ No

I have received and understand my responsibilities under Exhibits A, B, C and D. ☐ Yes ☐ No

I have received and understand my security responsibilities as outlined in the Access Security Requirements as provided by DFI with regard to consumer reports received. ☐ Yes ☐ No

Do you understand that your company <u>cannot resell information obtained by DFI</u>? ☐ Yes ☐ No

Are you, or your business, associated or affiliate with any of the following? ☐ Yes ☐ No

Adoption firm, Adult Entertainment, Asset Location, Attorney/Paralegal firm, Bail Bonds/Bounty Hunter, Check Cashing, Child Location Svc, Child Collection Support, Condominium/Homeowners Assoc., Country Club, Credit Counseling For Profit, Credit Repair/Credit Clinic, Dating Service, Debt Relief Products, Diet Centers, Financial Counseling, Foreign Company, Future Services – Health Clubs/Continuity Clubs, Genealogical Research, Insurance Claims, Internet People Locator, Judgment Recovery Entity, Law Enforcement, Legal Services, Loan Modification, Media / News/ Journalist, Massage Service, Other Reseller, Pawn Shop, Private Investigation, Repossession Company, Subscriptions, Spiritual Counseling, Tattoo Service, Timeshare, Weapons Dealer - Seller or Distributor.

If yes, please list services:_____

Does your company offer debt relief or mortgage assistance relief assistance products or services? ☐ Yes ☐ No

Has your company or any employee known to have been involved in credit fraud or other unethical business practice? ☐ Yes ☐ No

COMPANY NAME: _____

Print name of Owner/Officer: _____ **Title:** _____

AUTHORIZED SIGNATURE: _____ **Date:** _____

All documents must be physically signed.

MASTER SERVICE AGREEMENT – BANKING AND TENANT SOLUTIONS

This Master Service Agreement ("Agreement") is made between _____ ("User") and Data Facts, Inc. ("Data Facts"), subject to the following terms and conditions:

CERTIFICATION OF FCRA PERMISSIBLE PURPOSE
User certifies that all of its requests and procurement orders for consumer information from Data Facts will be made and the resulting reports will be used, for the following federal Fair Credit Reporting Act (FCRA), (15 U.S.C. § 1681 et seq), as amended by the Consumer Credit Reporting Reform Act of 1996, hereinafter called 'FCRA". Subscriber certifies it will use credit information for the following reasons as allowed by the FCRA and its permissible purpose is :

Mortgage Prescreening: _____Initial Here

1. COMPLIANCE WITH CONSUMER PROTECTION LAWS. A variety of state and federal laws, including the Fair Credit Reporting Act (FCRA) govern the use of the information procured from consumer reporting agencies. The User warrants that it shall comply with all state, federal and local laws, regulations and ordinances including but not limited to the FCRA, Equal Employment Opportunity Commission (EEOC) (Title VII of the Civil Rights Act of 1964, ECOA and Reg B. regarding the use, disclosure, protection, storage, retention, and destruction of the information received from Data Facts. The parties acknowledge that Data Facts does not provide legal advice. Instead, Data Facts encourages all Users to consult with their counsel regarding the restrictions and requirements of the FCRA. Data Facts suggest that the User work with its counsel to ensure that its policies and procedures related to the use of information obtained from Data Facts are in compliance with applicable state and federal laws. USER UNDERSTANDS THAT 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

2. SPECIFIC STATE INFORMATION

2.1 California Law Certification:
User will refer to **Exhibit A** in making the following certification and User agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act.
Please check ("X") the appropriate line below:

User certifies it ☐ IS or ☐ is NOT a "retail seller", as defined in Section 1802.3 of the California Civil Code and ☐ DOES or ☐ DOES NOT issue credit to consumers who appear in person on the basis of an application for credit submitted in person.

2.2 Vermont Certification: User certifies that it will comply with applicable provisions under Vermont law. In particular, User certifies that it will order information services relating to Vermont residents that are consumer reports as defined by the Vermont Fair Credit Reporting Act ("VFCRA"), only after User has received prior consumer consent in accordance with VFCRA section 2480e and applicable Vermont Rules. User further certifies that the attached copy of Section 2480e (**Exhibit B**) of the Vermont Fair Credit Reporting Statute was received from Data Facts, Inc.

3. CONFIDENTIALITY AND USE OF INFORMATION. User certifies that User shall use the consumer reports: (a) solely for the User's certified use(s); and (b) solely for the User's exclusive one-time use. User shall not request, obtain or use consumer reports for any other purpose including, but not limited to, for the purpose of selling, leasing, renting or otherwise providing information obtained under this Agreement to any other party, whether alone, in conjunction with User's own data, or otherwise in any service which is derived from the consumer reports. The consumer reports shall be requested by, and disclosed by User only to User's designated and authorized employees having a need to know and only to the extent necessary to

enable User to use the Consumer Reports in accordance with this Agreement. User shall ensure that such designated and authorized employees shall not attempt to obtain any consumer reports on themselves, associates, or any other personal except in the exercise of their official duties.

User shall use each consumer report only for a one-time use and shall hold the report and all consumer information, whether oral or written in strict confidence, and not disclose it to any third parties; provided, however, that User may, but is not required to, disclose the report to the subject of the report only in connection with an adverse action based on the report. No information will be requested for the use of any other person except with Data Facts' written permission. No information obtained through Data Facts to include but not limited to information from Equifax, Experian or Trans Union will be resold to any third party.

Any request for information by the person, or their representatives on which Data Facts prepares information, may be referred to Data Facts, Inc. or repository containing this information as notated on our report, for disclosure purposes as provided under the FCRA or other applicable laws.

3.1 Information Security Program: User 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 Data Facts; 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 Data Facts, (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.

3.2 Access Security Requirements User shall comply with all access security requirements imposed by Data Facts which are attached to this Agreement and incorporated by reference as a part of this Agreement. Users failure to comply with, such provision shall constitute a material breach of this agreement. User will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry. User agrees to properly store or dispose of all sensitive consumer information that will protect against unauthorized access or use of that information.

4. **AUDITS** Data Facts or its agents may periodically conduct audits of User regarding its compliance with the FCRA and other certifications in this Agreement. Audit will be conducted by email whenever possible and will require User to provide documentation as to permissible use of particular information. User gives its consent to Data Facts to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or User's material breach of this Agreement, constitute grounds for immediate termination of this Agreement. If Data Facts terminates this Agreement due to the conditions in the preceding sentence, User (i) unconditionally releases and agrees to hold Data Facts and its agents harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or relate to such termination, and (ii) covenants it will not assert any claim or cause of action of any kind or nature against Data Facts or its agents in connection with such termination.

5. **SITE INSPECTIONS**: A site inspection must be performed at the principle place of business of all Users. A third party vendor hired to act on our behalf will perform the site inspection. The purpose of the inspection is to ensure that the User's business facility is commensurate with the size and purported type of business listed on the membership application and the identifications and certifications made by the User. In the event the User's principle place of business changes, an additional site inspection must be performed. You must contact Data Facts immediately of such change.

6. INDEMNIFICATION. User agrees to hold Data Facts, Inc and their officers, employees and independent contractors and its agents (to include but not limited to Equifax, Experian and Trans Union) and their officers, employees and independent contractors harmless on account of any expense or damage resulting from the publishing by User, its employees or agents report information in a manner that is contrary to these conditions.

7. DISCLAIMER OF WARRANTY/LIMITATION OF LIABILITY Recognizing that information is secured by and through fallible human sources that for the fee charged Data Facts cannot be an insurer of the accuracy of the information. User understands and agrees that the accuracy of any information furnished is not guaranteed by Data Facts or its agents (to include but not limited to Equifax, Experian and Trans Union) and therefore User releases Data Facts, its officers, employees and independent contractors and their officers, employees and independent contractors from any liability or negligence in connection with the preparation of

such reports and from any loss or injury to our company resulting from the obtaining or furnishing of such information, and further agree to hold Data Facts, its officers, employees and independent contractors and its agents (to include but not limited to Equifax, Trans Union and Experian), and their officers, employees and independent contractors harmless and indemnify them from any and all claims, losses, and damages arising out of alleged liability suffered by User resulting directly or indirectly from the reports. Recognizing that a complete and accurate application or request is necessary for the preparation of an accurate report, the User releases Data Facts and their officers, employees, independent contractors and it's agents (to include but not limited to Equifax, Trans Union and Experian) and their officers, employees, and independent contractors from any liability for negligence in connection with the preparation of reports and from any loss or expense suffered by the User as a result of any intentional or unintentional failure to disclose all relevant personal, public record and credit history information by the User. The parties agree that Data Facts or its agents (to include but not limited to Equifax, Experian and Trans Union) shall not be liable for any special, indirect, incidental, punitive or consequential damages, including loss of profits, arising from or related to (i) the User's use of the reports provided by Data Facts or (ii) any acts or omissions of Data Facts. Data Facts' liability under this Agreement shall be limited to direct damages not to exceed the amounts actually received by Data Facts in the three months prior to the date of the action giving rise to the action.

8. PAYMENT REQUIREMENTS/COLLECTION. User will pay Data Facts' charges for the services rendered to User within fifteen (15) days of its receipt of the monthly invoice unless other arrangements are made in writing with an authorized Data Facts' officer. Data Facts reserves the right to charge a late fee on any outstanding account that is past due fifteen days or more. Such charge shall not exceed 1.5% per month on the outstanding balance or the maximum amount permitted to be charged by law, whichever is less. All past due accounts will be placed on hold until payment is received. A reconnect fee of $35 will be charged to reactive the account. In the event that legal action is necessary to obtain the payment of any amounts owed to Data Facts, the User shall pay all reasonable attorneys' fees and all other cost incurred by Data Facts in collection of such amounts. User has ninety (90) days from the date of invoice to notify Data Facts of any dispute with the invoice after which the invoice will be deemed accepted in all respects.

9. ARBITRATION AND TIME FOR FILING CLAIMS. Except for a claim made by Data Facts to collect on an outstanding account, any controversy or claim arising out of or relating to this Agreement shall be settled by arbitration in Memphis, Tennessee by a single arbitrator, in accordance with the Commercial Arbitration Rules of the American Arbitration Association, and a judgment upon the arbitration award may be entered in any court having jurisdiction. Notwithstanding what any statute of limitation may otherwise provide, the parties agree that no claim or right of action of any kind shall be asserted against Data Facts by the User unless such action is instituted by the User within six (6) months of the date that the transaction or occurrence giving rise to such claim or right of action took place regardless of when the User may have discovered the existence of such claim against Data Facts.

10. ATTORNEYS' FEES AND COSTS. In the event a dispute arises between the parties with respect to any matter related directly or indirectly to this Agreement, the party prevailing in such dispute shall be entitled to recover all expenses, including, without limitation, reasonable attorneys' fees and expenses incurred in ascertaining such party's rights, and in preparing to enforce, or in enforcing such party's rights under this Agreement, whether or not it was necessary for such party to institute suit or submit the dispute to arbitration. User further agrees to pay any and all fees, including attorney and court costs, which may be incurred in the collection of this account.

11. GOVERNING LAW. This Agreement shall be governed by Tennessee law.

12. SUCCESSORS. This Agreement shall inure to the benefit of and bind the successors, and assigns of the parties. User will promptly notify Data Facts in writing of any of the following events, change in User ownership, merger, acquisition name change, or a material change in nature of User's business.

13. TERM. This agreement shall remain in effect for one year from the date that it becomes effective after signature by both parties, and it shall automatically renew each year thereafter for an additional one-year term, unless one party notifies the other party in writing at least 10 days prior to termination of the Agreement. Data Facts shall have the right to terminate this Agreement immediately upon the occurrence of any of the following events: (a) the User fails to pay its invoices according to their terms; (b) the User breaches any of the other obligations imposed on it by the terms of this Agreement or (c) a material change in existing

legal requirements that adversely affects User's Agreement. Termination of this agreement shall not affect any executor provisions of this Agreement. The terms set forth in paragraphs 3, 6,7 9, 10, 11 and 12 shall expressly survive termination and be enforceable just as if the entire Agreement remained in effect. User understands and agrees that this Agreement constitutes all conditions of service and of reporting, present and future and applies to all reports made by Data Facts and its affiliated companies or branches to User at its Home Office or to any of its branches or service offices. No changes in these conditions may be made except by consent of an officer of Data Facts, Inc.

14. **Mortgage Underwriting Review/LQI/ Additional Pull Services-**Subscriber certifies that: (i) it will use the Additional Pull Service provided by Data Facts solely for the purpose of reviewing the credit Information of a consumer with a pending mortgage loan with the Subscriber to determine, prior to closing the pending mortgage loan, whether the consumer has any potential increase in debt and funding and will not use the Additional Pull Service for any other purpose, (ii) it will not use an AP Member Number except in connection with a prior request from the same Qualified Subscriber with a CRA ZB member number that causes a "Hard Inquiry" to be posted in the consumer's credit file (the initial request must be made by the Qualified Subscriber not a third party such as a third party loan originator), (iii) the prior request will have been made through Data Facts, not a different consumer reporting agency, and (iv) the Qualified Subscriber will not use the additional Data Facts Credit Information to make a new underwriting decision but rather will make a new request for Data Facts Credit information.

15. **Death Master File –**

TransUnion: 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). As many credit repository services contain information from the DMF, the credit repositories would like to remind you of your continued obligation to restrict your use of deceased flags or other indicia within the repository 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. Adverse action against any consumer should not take place without further investigation to verify the information from the deceased flags or other indicia from these services. User certifies that it meets the qualifications of a Certified Person under 15 CFR Part 1110.2 and that its access to the DMF is appropriate because:

a. **Certified Person:** End User has a legitimate fraud prevention interest, or has a legitimate business purpose pursuant to a law, governmental rule, regulation or fiduciary duty, and shall specify the basis for so certifying; and

b. **Security:** End User has systems, facilities, and procedures in place to safeguard the accessed information; experience in maintaining the confidentiality, security, and appropriate use of the accessed information, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986; and agrees to satisfy the requirements of such section 6103(p)(4) as if such section applied to End User; and

c. End User shall not disclose information derived from the DMF to the consumer or any third party, unless clearly required by law.

d. **Penalties:** End User acknowledges that failure to comply with the provisions above may subject Reseller to penalties under 15 CFR 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year.

e. **Indemnification and Hold Harmless:** End User shall indemnify and hold harmless Data Facts, TransUnion, and the U.S. Government/NTIS from all claims, demands, damages, expenses, and losses, whether sounding in tort, contract or otherwise, arising from or in connection with End User's, or End User's employees, contractors, or subcontractors, use of the DMF. This provision shall survive termination of the Agreement and will include any and all claims or liabilities arising from intellectual property rights

f. Liability:

a. Neither Data Facts, TransUnion nor the U.S. Government/NTIS (a) make any warranty, express or implied, with respect to information provided under this Section of the Policy, including, but not limited to, implied warranties of merchantability and fitness for any particular use; (b) assume any liability for any direct, indirect or consequential damages flowing from any use of any part of the DMF, including infringement of third party

intellectual property rights; and (c) assume any liability for any errors or omissions in the DMF. The DMF does have inaccuracies and NTIS and the Social Security Administration (SSA), which provides the DMF to NTIS, does not guarantee the accuracy of the DMF. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on the DMF is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the DMF.

b. If an individual claims that SSA has incorrectly listed someone as deceased (or has incorrect dates/data on the DMF), the individual should be told to contact to their local Social Security office (with proof) to have the error corrected. The local Social Security office will:

I Make the correction to the main NUMIDENT file at SSA and give the individual a verification document of SSA's current records to use to show any company, recipient/purchaser of the DMF that has the error; OR,

ii. Find that SSA already has the correct information on the main NUMIDENT and DMF (probably corrected sometime prior), and give the individual a verification document of SSA's records to use to show to any company subscriber/ purchaser of the DMF that had the error.

Experian: 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.

16. **Social Security Administration requirements for verification of SSNs** - The Requesting Party acknowledges the following: Section 1140 of the Social Security Act, authorizes SSA to impose civil monetary penalties on any person who uses the words "Social Security" or other program- related words, acronyms, emblems and symbols in connection with an advertisement, solicitation or other communication,, in a manner which such person knows or should know would convey, or in a manner which reasonably could be interpreted or construed as conveying, the false impression that such item is approved, endorsed, or authorized by the Social security Administration…" 42 U.S.C. 1320b-10(a). Requesting Party, or any of its Principals, is specifically prohibited from using the words "Social Security" or other CBSV program-related words, acronyms, emblems and symbols in connection with an advertisement for "identity verification." Requesting Party, or any of its Principals, is specifically prohibited from advertising that SSN verification provides or serves as identity verification. SSA has the right to review the Requesting Party's or any of its Principal's records associated with the CBSV program at any time. Note: These acknowledgements shall extend to Principals with that are not the Requesting Party. The information obtained from records maintained by SSA is protected by Federal statutes and regulations, including 5 U.S.C. 552a(i)(3) of the Privacy Act. Under this section, any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses will be guilty of a misdemeanor and fined not more than $5,000.

17. SERVICES PROVIDED Data Facts agrees to furnish reporting services to users in accordance with the terms of this Agreement. While Data Facts will attempt to provide its services in the most efficient manner possible, Data Facts shall have no liability to User for any delay or failure to deliver consumer reports caused by a third party that provides data or information to Data Facts.

This Agreement set forth the entire understanding of the parties with respect to the subject matter hereof and supersede to the extent indicated all prior agreements, letters, covenants, arrangements, communications, representations and warranties, whether oral or written, by an employee, officer or representative of their party.

REQUIRED DOCUMENTS: Consumer Reporting Agencies are required to provide Users of consumer reports the CFPB prescribed notices. User acknowledges receipt of these two (2) documents: "Summary of Rights" (EXHIBIT C) and the Notice of Users of Consumer Reports: Obligations of Users under the FCRA (EXHIBIT D). If User does not have a copy of these documents, call the Data Facts office.

Signature of Agreement for Services

Date: _____

Signed by: _____

Print Name: _____

Title: _____

Date: _____

Signed by: _____

Print Name: _____

Title: _____

My signature indicates I have direct knowledge of the facts certified in this agreement

Company: _____

Signors Physical Location:
_____
_____

Data Facts, Inc.
PO BOX 4276
Cordova, TN 38088

CREDIT SCORING SERVICES AGREEMENT
MORTGAGE/BANKING/REAL ESTATE/TENANT

This Credit Scoring Services Agreement dated _____ is between _____ (customer) and Data Facts, Inc.

A. Subject of Agreement. The subject of this Agreement is customer's purchase of certain credit scoring services known as the "Experian/Fair Isaac Model" from Experian/Fair Isaac, The "Beacon" model developed by Fair Isaac and Equifax, and the "Fico Classic and/or Empirica" models developed by Fair Isaac and Trans Union (collectively risk scoring models).

B. Application. This Agreement applies to all uses of any risk scoring model provided by Experian, Equifax and/or Trans Union accessed through and offered by Data Facts, Inc., its agents, affiliates, assigns or any third party involved in the delivery of any scoring model.

C. Meaning of Risk Scoring Models. For purposes of this Agreement, the term "risk scoring models" means application of a risk model developed by Fair, Isaac and Company and Experian and/or Equifax and/or Trans Union of which each employs a proprietary algorithm and which, when applied to credit information relating to individuals with whom the End User (customer) has a credit relationship or with whom the End User (customer) contemplates entering into a credit relationship will result in a numerical score (the Score); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment. Data Facts, Inc. reasonably believes that, subject to validation by customer on its own records, (1) the scoring algorithms used in computation of the Score(s) are empirically derived from consumer credit information from Experian's, Equifax's and/or Trans Union's databases, and are demonstrably and statistically sound methods of rank ordering candidate records from said databases for the purposes for which the Score(s) was designed.

D. Release. The information including, without limitation, the consumer credit data, used in providing Scores under this Agreement were obtained from sources considered to be reliable. However, due to the possibilities of errors inherent in the procurement and compilation of data involving a large number of individuals, neither the accuracy nor completeness of such information is guaranteed. Data Facts, Inc., nor Experian, nor Equifax, nor Trans Union guarantee the predictive value of the Score(s) with respect to any individual and do not intend to characterize any individual as to credit capability. Neither Data Facts, Inc., nor Experian, nor Equifax, nor Trans Union nor any respective directors, officers, employees, agents, subsidiaries, affiliated companies or bureaus or any third party contractors, licensors or suppliers of Data Facts, Inc, Experian, Equifax and/or Trans Union will be liable to customer for any claim, injuries, damages, losses, costs or expenses incurred or suffered directly or indirectly by customer resulting from any inaccuracy or incompleteness of such information used in providing Scores under this Agreement and/or as a result of customer's use of Scores and/or failure of a Score(s) to accurately predict the credit worthiness of customer's applicants or customers and/or any other information or services provided under this Agreement.

E. Permissible Purpose. Customer warrants that it has a permissible purpose under the Fair Credit Reporting Act, as it may be amended from time to time, to obtain the information derived from the Experian/Fair Isaac Model, the Equifax /Fair Isaac Model and/or the Trans Union/Fair Isaac Model and will use the Scores obtained for no other purpose.

F. Experian, and/or Equifax, and/or Trans Union, and/or Fair Isaac shall all be deemed third party beneficiaries under this Agreement.

G. Disclosure of Scores. Customer will request and use Scores and reason codes solely for customer's own one time use. Customer may store Scores solely for Customer's own use in furtherance of customer's original purpose for obtaining the Scores. Customer will hold all information received from or through Data Facts, Inc., Experian, Equifax and/or Trans Union in connection with any score(s) and/or principal factors contributing to the Score(s) in strict confidence and will not disclose that information to the applicant or to others except as required or permitted by law.

H. Compliance and Confidentiality. In performing this Agreement and in using information provided hereunder, both parties will comply with all Federal, state, and local statutes, regulations and rules applicable to consumer credit information and Scores and nondiscrimination in the extension of credit from time to time in effect during the Term. All Scores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible in whole or in part, to any Person except to those employees of Customer with a need to know and in the course of their employment or to those third party processing agents of Customer who have

executed a written agreement that limits the use of the Scores by the third party to the use permitted to Customer and contains the prohibitions set forth herein regarding model development, model calibration and reverse engineering or when accompanied by the corresponding reason codes, to the consumer who is the subject of the Score; or as required by law and that such third party shall utilize Scores for the sole benefit of Customer and shall not utilize the Scores for any other purpose including for such third party's own purpose or benefit. Such third party shall not resell Scores and such third party shall not use the Scores to create or maintain a database for itself or otherwise. Without limiting the generality of the foregoing, each party will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of either party and while in transport between the parties.

I. **Successors.** This Agreement shall be binding upon and inure to the benefit of the successors of each of the parties hereto, but shall not be assignable by customer without the prior written consent of Data Facts, Inc.

J. **Proprietary Criteria.** Under no circumstances will customer or any End User attempt in any manner, directly or indirectly, to use the Scores for model development or model calibration nor attempt to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian, Equifax, Trans Union, Data Facts, Inc. and/or Fair, Isaac.

K. **Prohibition.** Under no circumstances will customer, its employees, agents or subcontractors use in any manner the trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered of Experian Information Solutions, Inc, Equifax, Trans Union, Data Facts or Fair Isaac and Company, or the affiliates of any of them, or of any other party involved in the provision of the Experian/Fair Isaac model, Equifax/Fair Isaac Model, or Trans Union/Fair Isaac model without such entity's prior written consent.

L. **Punitive Damages.** In no event shall any party be liable for any consequential, incidental, indirect, special, or punitive damages incurred by the other parties and arising out of the performance of this agreement, including but not limited to loss of good will and lost profits or revenue, whether or not such loss or damage is based in contract, warranty, tort, negligence, strict liability, indemnity, or otherwise even if a party has been advised of the possibility of such damages, these limitations shall apply notwithstanding any failure of essential purpose of any limited remedy. The foregoing notwithstanding, with respect to customer, in no event shall the aforestated limitations of liability, set forth above apply to damages incurred by Data Facts, and/or Experian, and/or Equifax, and/or Trans Union, and/or Fair Isaac as a result of governmental, regulatory or judicial action(s) to the extent such damages result from customer's breach, directly or through customer's agent(s) of its obligations under this agreement. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF PROVIDER, EXPERIAN OR FAIR, ISAAC TO END USER EXCEED THE FEES PAID BY END USER PURSUANT TO THIS AGREEMENT DURING THE SIX MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF END USER'S CLAIM.

M. **Experian Warranty.** Experian/Fair Isaac warrants that the Experian/Fair Isaac Model is empirically derived and demonstrably and statistically sound and that to the extent the population to which the Experian/Fair Isaac model is applied is similar to the population sample on which the Experian/Fair Isaac Model was developed, the Experian/Fair Isaac Model score may be relied upon by Customer and/or end Users to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to End User. Experian/Fair Isaac further warrants that so long as it provides the Experian/Fair Isaac Model, it will comply with regulations promulgated from time to time pursuant to the Equal Credit Opportunity Act 15 USC Section 1691 et seq. The foregoing warranties are the only warranties Experian/Fair Isaac have given customer and/or End Users with respect to the Experian/Fair Isaac model and such warranties are in lieu of all other warranties express or implied, Experian/Fair Isaac might have given customer and/or End Users with respect thereto, including, for example warranties of merchantability and fitness for a particular purpose. Customer and each respective end user's rights under the foregoing warranty are expressly conditioned upon each respective end user's periodic revalidation of the Experian/Fair Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 et seq.).

N. **Trans Union required information.** Fair Isaac, the developer of Classic, warrants that the scoring algorithms as delivered to Trans union and used in the computation of the Class Scores ("Models") are empirically derived from Trans union's credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring when applied to the population for which they were developed, and that no scoring algorithm used by Classic uses a "prohibited basis" as that term is defined in the Equal Credit Opportunity Act (ECOA) and regulation B promulgated hereunder. Classic provides a statistical evaluation of certain information in Trans union's files on a particular individual and the Classic Score indicates the

relative likelihood that the consumer will repay their existing or future credit obligations satisfactorily over the Twenty-Four (24) month period following scoring relative to other individuals in Trans Union's data base. The score may appear on a credit report for convenience only, but is not part of the credit report nor does it add to the information in the report on which it is based.

Trans Union required information. The warranties set forth in section L are the sole warranties made under this agreement concerning the Classic scores and any other documentation or other deliverables and services provided under this agreement; and neither Fair Isaac nor Trans union make any other representations or warranties concerning the products and services to be provided under this agreement other than set forth in this agreement. The warranties and remedies set forth in section L are in lieu of all others, whether written or oral, express or implied (including, without limitation, warranties that might be implied from a course of performance or dealing or trade usage). There are no implied warranties of merchantability or fitness for a particular purpose. Additionally, neither Trans union nor Fair Isaac shall be liable for any and all claims arising out of or in connection with this agreement brought more than one 91) year after the cause of action has accrued. In no event shall Trans Union's and Fair Isaac's aggregate total liability, if any, under this agreement exceed the aggregate amount paid under this agreement, by customer during the twelve (12) month period immediately preceding any such claim, or ten thousand dollars ($10,000) whichever amount is less.

O. Term and Cancellation. The term of this Agreement (the "Term") is the period consisting of the Initial Term and, if this Agreement is renewed, the Renewal Term(s) as follows:

(1) Initial Term. The "initial term" is the period beginning at 12:01 a.m. on the date written above and ending at 11:59 p.m. on the day before the anniversary of that date.

(2) Renewal Term(s) Unless one or both of the parties delivers written notice of such party's (parties') intent not to renew no later than thirty (30) days before the end of the Initial Term, this Agreement will renew automatically and without further action by either party for an additional one-year period (a "Renewal Term"). Thereafter, this Agreement will continue to renew automatically unless and until either party delivers non-renewal notice no later than thirty (30) days before the end of a Renewal Term.

(3) Termination. This Agreement will terminate immediately and without further action by either of the parties in the event customer discontinues use of all risk scoring models, in the event of a breach of the provisions of this agreement by customer, in the event the agreement(s) related to Scores between Experian, and/or Equifax, and/or Trans Union, and/or Data facts, and/or Fair Isaac are terminated or expire, or in the event the requirements of any law, regulation or judicial action are not met, or as a result of changes in laws, regulations or regulatory of judicial action, that the requirements of any law, regulation or judicial action will not be met; and/or the use of the Score service is the subject of litigation or threatened litigation by any governmental entity. Otherwise, this agreement will terminate upon written notice by either party.

P. Complete Agreement. This Agreement sets forth the entire understanding of Customer and Data Facts, Inc. with respect to the subject matter hereof and supersedes all prior letters of intent, agreements, covenants, arrangements, communications, representations, or warranties, whether oral or written, by any officer, employee, or representative of either party relating thereto.

Additional Terms and Conditions for FICO Scores and Equifax VantageScores

1. From time to time, End User may request that Equifax, TransUnion or Experian provide FICO Scores (other than archive scores), for, in each case, one of the following internal decisioning purposes requested: (a) in connection with the review of a consumer report it is obtaining from Equifax, TransUnion or Experian ; (b) for the review of the portion of its own open accounts and/or closed accounts with balances owing that it designates; (c) as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; (d) for use as a selection criteria to deliver a list of names to End User or End User's designated third party processor agent; (e) for transactions not initiated by the consumer for the extension of a firm offer of credit or insurance; or (f) with respect to the insurance risk scores only for use in connection with the underwriting of insurance involving the consumer. End User shall use each such FICO Score only once and, with respect to FICO Scores other than archive scores, only in accordance with the permissible purpose under the FCRA for which End User obtained the FICO Score.

- End User may also request that TransUnion provide FICO Scores that utilize archived, depersonalized, consumer report information ('Archive Scores') and TransUnion agrees to perform such processing as reasonably practicable. End User shall use the Archive Scores solely to determine the validity of the FICO Scores for the benefit of End User for the single project for which the Archive Scores were acquired, but for no

other purpose and for no other entity. Determining validity of the FICO Scores consists solely of ; (a) internal validation on End User's own account performance data; (b) internal evaluation of the predictive strength of the FICO Scores as compared to other scores; (c) internal evaluation of the value of the FICO Scores as an internal component of custom models; and/or (d) establishing score cut-offs and strategies, as they relate to End User's portfolios. End User shall not make any attempt to link the Archive Scores to any information which identifies the individual consumers.

2. End User acknowledges that the FICO Scores are proprietary to Fair Isaac Corporation ('Fair Isaac') and that Fair Isaac retains all its intellectual property rights in the FICO Scores and the Models (defined below) used by Equifax, TransUnion or Experian to generate the FICO Scores. Fair Isaac grants to End User, effective during the term of the End User Agreement, a personal, non-exclusive, non-transferable, limited license to use, internally, the FICO Scores solely for the particular purpose set forth in Section 1 above for which the FICO Scores were obtained, including, but not limited to the single use restrictions set forth above. End User's use of the FICO Scores must comply at all times with applicable federal, state and local law and regulations, and End User hereby certifies that it will use each FICO Score (other than Archive Scores) only for a permissible purpose under the FCRA. End User shall not attempt to discover or reverse engineer, or similar or emulate the functionality of the FICO Scores, Models or other proprietary information of Fair Isaac, or use the FICO Scores in any manner not permitted under this Agreement, including, without limitation, for resale to third parties, model development, model validation (except as expressly set forth above in Paragraph 1 of this Agreement), model benchmarking, or model calibration or any other purpose that may result in the replacement of or discontinued use of the FICO Scores. "Model" means Fair Isaac's proprietary scoring algorithm(s) embodied in its proprietary scoring software delivered to and operated by Equifax, TransUnion or Experian.

3. End User shall not disclose the FICO Scores nor the results of any validations or other reports derived from the FICO Scores to any third party (other than to a consumer as expressly permitted in the Agreement and this Section 3) unless: (a) such disclosure is clearly required by law; (b) Fair Isaac, Equifax, TransUnion or Experian provides written consent in advance of such disclosure; and/or (c) such disclosure is to End User's designated third party processor agent; provided however that in either (i.e., (b) or (c) above) event, End User may make such disclosure (or in the event of (c), direct Equifax, TransUnion or Experian to deliver such lists), only after End User has entered into an Agreement with the third party that (i) limits use of the FICO scores to only the use permitted to End User hereunder, (ii) obligates the third party provider to otherwise comply with these terms, and (iii) names Fair Isaac as an intended third party beneficiary of such agreement with respect to the Models, FICO Scores, and other Fair Isaac intellectual property and fully enforceable rights. End User shall not disclose a FICO Score to the consumer to which it pertains unless such disclosure is (i) approved in writing by Fair Isaac or (ii) required by law or is in connection with an adverse action (as defined by the FCRA) and then only when accompanied by the corresponding reason codes.

4. Fair Isaac represents and warrants that the scoring algorithm(s) used in the Models to produce FICO Scores are empirically derived and demonstrably and statistically sound; provided, that, this warranty is conditioned on (i) an End User's use of each FICO Score for the purposes for which the respective Model was designed, as applied to the United States population used to develop the scoring algorithm, (ii) the End User's compliance with all applicable federal, state and local laws and regulations pertaining to the use of the FICO Scores, including the End User's duty (if any) to validate or revalidate the use of credit scoring systems under the ECOA and Regulation B, and (iii) the End User's use of the FICO Scores otherwise remaining in compliance with the terms of the Agreement with respect to FICO Scores. FOR ANY BREACH OF THIS WARRANTY, EDN USER'S SOLE AND EXCLUSIVE REMEDY, AND FAIR ISAAS'S, EQUIFAX, TRANSUNION AND EXPERIAN ENTIRE LIABILITY, SHALL BE RECALCUATIN OF THE FICO SCORES THAT FORMED THE BASIS OF SUCH BREACH. FAIR ISAAC, EQUIFAX, TRANSUNION AND EXPERIAN HEREBY DISCLAM ALL OTHER WARRANTIES, WHETHER STATUTORY, EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND OTHER WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR DEALING OR TRADE USAGE.

5. IN NO EVENT SHALL END USER, EQUIFAX TRANSUNION, EXPERIAN, OR FAIR ISAAC BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES INCURRED BY ANY PARTY AND ARISING OUT OF THE PERFORMANCE HEREUNDER, INCLUDING BUT NOT LIMITED TO LOSS OR GOODWILL AND LOST PROFITS OR REVENUE, WHETHER OR NOT SUCH LOSS OR DAMAGE IS BASED IN CONTRACT, WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, INDEMNITY,OR OTHERWISE, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF SUCH DAMAGES WERE REASONABLY FORESEEABLE. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. THE FOREGOING LIMITATIONS SHALL NOT APPLY TO FAIR ISAAC'S, EQUIFAX, TRANSUNION OR EXPERIAN'S VIOLATION OF END USER'S INTELLECTUAL PROPERTY RIGHTS NOR END USER'S VIOLATION OF EQUIFAX, TRANSUNION, EXPERIAN OR FAIR ISAAC'S INTELLECTUALPROPERTY RIGHTS (INCLUDING THE USE OR DISCLOSURE OF FAIR ISAAC SCORES IN VIOLATION OF THE TERMS OF THIS AGREEMENT) ADDITIONALY, NEITHER EQUIFAX, TRANSUNION, EXPERIAN NOR FAIR ISAAC SHALL BE LIABLE FOR ANY CLAIM ARISING OUT OF

OR IN CONNECTION WITH THIS AGREEMENT BROUGHT MORE THAN ONE (1) YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED. IN NO EVENT SHALL EQUIFAX, TRANSUNION, EXPERIAN AND FAIR ISAAC'S COMBINED AGGREGATE TOTAL LIABILITY HEREUNDER EXCEED THE AMOUNTS PAID HEREUNDER DURING THE PRECEDING TWELVE (12) MONTHS FOR THE FICO SCORES THAT ARE THE SUBJECT OF THE CLAIM(S) OR TEN THOUSAND DOLLARS ($10,000), WHICHEVER AMOUNT IS LESS.

6. Upon prior written notice, Equifax, TransUnion, Experian and Fair Isaac shall have the right to audit End User to verify End User's compliance with this Agreement. End User shall accommodate Equifax, TransUnion, Experian and Fair Isaac in connection with such audit. Such accommodation shall include, but not be limited to on-site inspection of End User's records, systems and such documentation as deemed reasonably necessary to demonstrate compliance with this Agreement. Equifax, TransUnion or Experian and End User acknowledge and agree that Fair Isaac is a third party beneficiary hereunder with respect to the Models, FICO Scores, and other Fair Isaac intellectual property and with fully enforceable rights. End User further acknowledges and agrees that Fair Isaac's rights with respect to the Models, FICO Scores, other Fair Isaac intellectual property, and all works derived therefrom are unconditional rights that shall survive the termination for any reason.

End User will comply with applicable federal and state laws, rules and regulations relating to such party's performance of its obligations under these Terms and Conditions including, but not limited to, all applicable consumer financial protection laws. In addition, End User shall not engage in any unfair, deceptive, or abusive acts or practices.

Additional Terms and Conditions Applicable to VantageScores
VantageScore is a tri-bureau credit risk model developed using one algorithm across sample data common to all three credit Bureaus. The following additional terms and conditions apply to End User's receipt and use of VantageScore:
End User Terms for VantageScore – End User will request VantageScores only for End User's exclusive use. End User may store VantageScores solely for End User's own use in furtherance of End User's original purpose for obtaining the VantageScores. End User shall not use the VantageScores for model development or model calibration, except in compliance with the following conditions: (1) the VantageScores may only be used as an independent variable in custom models; (2) only the raw archived VantageScore and VantageScore segment identifier will be used in modeling (i.e. no other VantageScore information including, but not limited to, adverse action reasons, documentation, or scorecards will be used); and (3) End User depersonalized analytics and/or depersonalized third party modeling analytics performed on behalf of End User, using VantageScores, will be kept confidential and not disclosed to any third party other than as expressly provided for below in subsections (ii), (iii), (iv), (v) and/or (vi) of this paragraph. End User shall not reverse engineer the VantageScore. All VantageScores provided hereunder will be held in strict confidence and may never be sold, licensed, copied, reused, disclosed, reproduced, revealed or made accessible, in whole or in part, to any person or entity, except (i) to those employees, agents , and independent contractors of End User with a need to know and in the course of their employment; (ii) to those third party processing agents and other contractors of End User who have executed an agreement that limits the use of the VantageScores by the third party only to the use permitted to End User and contains the prohibitions at least as restrictive as 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 VantageScore (provided that, accompanying reason codes are not required to the extent permitted by law); (iv) to government regulatory agencies; (v) to ratings agencies, dealers, investors and other third parties for the purpose of evaluating assets or investments (e.g. securities) containing or based on obligations of the consumers to which the VantageScore apply (e.g. mortgages, student loans, auto loans, credit cards), provided that as it relates to this subsection (v), (a) End User may disclose VantageScores only in aggregated formats (e.g. averages and comparative groupings) that do not reveal individual VantageScores, (b) End User shall not provide any information that would enable a recipient to identify the individuals to whom the VantageScores apply, and (c) End User shall enter into an Agreement with each recipient that limits the use of the

VantageScore to evaluation of such assets or investments, or (vi) as required by law. End User agrees that the trademarks, trade names, product names, brands, logos, and service marks ("Vantage Marks") for VantageScores and VantageScore credit scoring models will remain the sole property of VantageScore Solutions, LLC. End User obtains a limited, non-exclusive, non-transferable, royalty free license to use and display the Vantage Marks in connection with the activities solely permitted by the Agreement. The use of the Vantage Marks under the preceding license is limited to use only in connection with the Services covered by

this Agreement, and the End User expressly agrees not to use the Vantage Marks in connection with any products or services not covered by this Agreement. Any use of the Vantage Marks is subject to VantageScore Solutions, LLC's prior written authorization. End User further agrees it will include the Vantage Marks in all advertising and marketing materials which reference the VantageScores or Vantage models and it will comply with the VantageScore Trademark Policy and Brand Guidelines, which may be changed from time to time upon written notice. All use of the Vantage Marks will accrue solely to the benefit of VantageScore Solutions, LLC

Data Facts, Inc.

_____

(Print or type name of Customer)

By: _____

Name: _____

Title: _____

Date: _____

Address for Notice:

Data Facts, Inc

ATTN: Compliance
PO BOX 4276
Cordova, TN 38088

By: _____

Name: _____

Title: _____

Date:_____

Address for Notice:

_____
_____
_____
_____

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 through Data Facts, 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. Data Facts 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 Data Facts services, Company agrees to follow these Experian security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store Experian data:

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

1.1 All credentials such as User names/identifiers/account numbers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Data Facts will ever contact you and request your credentials.

1.2 If using third party or proprietary system to access Data Facts 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 Data Facts data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access Data Facts 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 Data Facts 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. user/account 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 disclosed to an unauthorized party (see section 4.3 for reporting requirements)

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.

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.

3.5 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 Data Facts 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 the Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian's list of compliant service providers. If the service provider is in the process of becoming compliant, it is Company's responsibility to ensure the service provider is engaged with Experian and an 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.

5.3 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 Data Facts 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 Data Facts 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.

7.6 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 Data Facts 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 Data Facts 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 Data Facts 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 Data Facts 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 Data Facts systems shall be made available to Data Facts upon request, for example during breach investigation or while performing audits.

8.6 Data requests from Company to Data Facts 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 Data Facts within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to Data Facts 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 800-264-4110, Email notification will be sent to support@datafacts.com .

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 Data Facts 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 Data Facts networking and computing resources may be monitored and audited by Data Facts, 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 Data Facts 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 Data Facts.

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."

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 Data Facts 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 Data Facts on systems access related matters. The Company's Head Security Designate will be responsible for establishing, administering and monitoring all Company employees' access to Data Facts 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 Data Facts product based upon the legitimate business needs of each employee. Data Facts 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 Data Facts. 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). Data Facts approval of requests for (Internet) access may be granted or withheld in its sole discretion. Data Facts 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 Data Facts 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 Data Facts 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 Data Facts on information and product access, in accordance with these Experian Access Security Requirements for Reseller End-Users. 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 Data Facts systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to Data Facts immediately.
2. As a Client to Data Facts products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
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 Data Facts 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 Data Facts Security Administration group on information and product access matters.

4. The Head Designate shall be responsible for notifying their corresponding Data Facts 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 Data Facts 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 Data Facts regarding access to Data Facts products and services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Data Facts.
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 Data Facts when needed on any system or user related matters.

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.
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.
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.

Company Name: _____ Account #: _____

Company Representative: _____

Position/Title: _____ Date _____

EXHIBIT A
END USER CERTIFICATION OF COMPLIANCE
California Civil Code - Section 1785.14(a)

Section 1785.14(a), as amended, states that a consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will only be used for a permissible purpose unless all of the following requirements are met:

Section 1785.14(a)(1) states: "If a prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the consumer credit reporting agency shall, with a reasonable degree of certainty, match at least three categories of identifying information within the file maintained by the consumer credit reporting agency on the consumer with the information provided to the consumer credit reporting agency by the retail seller. The categories of identifying information may include, but are not limited to, first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number. The categories of information shall not include mother's maiden name."

Section 1785.14(a)(2) states: "If the prospective user is a retail seller, as defined in Section 1802.3, and intends to issue credit to a consumer who appears in person on the basis of an application for credit submitted in person, the retail seller must certify, in writing, to the consumer credit reporting agency that it instructs its employees and agents to inspect a photo identification of the consumer at the time the application was submitted in person. This paragraph does not apply to an application for credit submitted by mail."

Section 1785.14(a)(3) states: "If the prospective user intends to extend credit by mail pursuant to a solicitation by mail, the extension of credit shall be mailed to the same address as on the solicitation unless the prospective user verifies any address change by, among other methods, contacting the person to whom the extension of credit will be mailed."

In compliance with Section 1785.14(a) of the California Civil Code, _____ ("End User") hereby certifies to Consumer Reporting Agency as follows: (Please circle)

End User ***(IS) (IS NOT)*** a retail seller, as defined in Section 1802.3 of the California Civil Code ("Retail Seller") and issues credit to consumers who appear in person on the basis of applications for credit submitted in person ("Point of Sale").

End User also certifies that if End User is a Retail Seller who conducts Point of Sale transactions, End User will, beginning on or before July 1, 1998, instruct its employees and agents to inspect a photo identification of the consumer at the time an application is submitted in person.

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

If End User is not a Retail Seller who issues credit in Point of Sale transactions, End User agrees that if it, at any time hereafter, becomes a Retail Seller who extends credit in Point of Sale transactions, End User shall provide written notice of such to Consumer Reporting Agency prior to using credit reports with Point of Sale transactions as a Retail Seller, and shall comply with the requirements of a Retail Seller conducting Point of Sale transactions, as provided in this certification.

EXHIBIT B

VERMONT FAIR CREDIT REPORTING STATUTE, 9 V.S.A. § 2480e (1999)

§ 2480e. Consumer Consent

(a) A person shall not obtain the credit report of a consumer unless:

(1) the report is obtained in response to the order of a court having jurisdiction to issue such an order; or

(2) the person has secured the consent of the consumer, and the report is used for the purpose consented to by the consumer.

(b) Credit reporting agencies shall adopt reasonable procedures to assure maximum possible compliance with subsection (a) of this section.

(c) Nothing in this section shall be construed to affect:

(1) the ability of a person who has secured the consent of the consumer pursuant to subdivision (a)(2) of this section to include in his or her request to the consumer permission to also obtain credit reports, in connection with the same transaction or extension of credit, for the purpose of reviewing the accounts, increasing the credit line on the account, or for other legitimate purposes associated with the account; and

(2) the user of credit information for the purpose of prescreening, as defined and permitted from time to time by the Federal Trade Commission.

VERMONT RULES ***
AGENCY 06. OFFICE OF THE ATTORNEY GENERAL
SUB-AGENCY 01. CONSUMER PROTECTION DIVISION
CHAPTER 012. Consumer Fraud -- Fair Credit Reporting
RULE CF 112 FAIR CREDIT REPORTING
CVR 06-031-012, CF 112.03 (1999)
CF 112.03 CONSUMER CONSENT

(a) A person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing if the consumer has made a written application or written request for credit, insurance, employment, housing or government benefit. If the consumer has applied for or requested credit, insurance, employment, housing or government benefit in a manner other than in writing, then the person required to obtain consumer consent pursuant to 9 V.S.A. §§ 2480e and 2480g shall obtain said consent in writing or in the same manner in which the consumer made the application or request. The terms of this rule apply whether the consumer or the person required to obtain consumer consent initiates the transaction.

(b) Consumer consent required pursuant to 9 V.S.A. §§ 2480e and 2480g shall be deemed to have been obtained in writing if, after a clear and adequate written disclosure of the circumstances under which a credit report or credit reports may be obtained and the purposes for which the credit repot or credit reports may be obtained, the consumer indicates his or her consent by providing his or her signature.

(c) The fact that a clear and adequate written consent form is signed by the consumer after the consumer's credit report has been obtained pursuant to some other form of consent shall not affect the validity of the earlier consent.

EXHIBIT C

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 CFPB'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 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 prepayment 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 "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 as 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 identify 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 extended fraud 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 are available at www.consumerfinance.gov/learnmore.

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 CFPB.

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 the 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 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 subjects 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 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. 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 EMPLOYMEE 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 are not treated as consumer reports so lon as the employer or its agent complies with the procedures set forth 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 regulations) the consumer must provide specific written consent and the medical information must be relevant. Any user who receives medical information shall not disclose the information to any other person (except where necessary to carry out the purpose for which the information was disclosed, or a 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. Sections 603(1), 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. The statement must include the address and toll-free telephone number of the appropriate notification system.

In addition, 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. <u>Disclosure and Certification Requirements</u>

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 identify 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.

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 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. 1681c-A
Section 605B	15 U.S.C. 1681c-B
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. 1681l
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. 16

EXHIBIT D

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 the 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 from the lists these offers are based on. You may opt-out with the nationwide credit bureaus at 1-888-5OPTOUT (1-888-567-8688).

• **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.	a. Consumer Financial Protection Bureau 1700 G Street NW Washington, DC 20552
b. Such affiliates that are not banks, savings associations, or credit unions also should list, in addition to the CFPB:	b. Federal Trade Commission: Consumer Response Center – FCRA Washington, DC 20580 (877) 382-4357
2. To the extent not included in item 1 above:	a. Office of the Comptroller of the Currency Customer Assistance Group 1301 McKinney Street, Suite 3450 Houston, TX 77010-9050
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	b. Federal Reserve Consumer Help Center P.O. Box 1200 Minneapolis, MN 55480
c. Nonmember Insured Banks, Insured State Branches of Foreign Banks, and insured state savings associations	c. FDIC Consumer Response Center 1100 Walnut Street, Box #11 Kansas City, MO 64106
d. Federal Credit Unions	d. National Credit Union Administration Office of Consumer Protection (OCP) Division of Consumer Compliance and Outreach (DCCO) 1775 Duke Street Alexandria, VA 22314
3. Air carriers	General Counsel for Aviation Enforcement & Proceedings Aviation Consumer Protection Division Department of Transportation 1200 New Jersey Avenue, SE Washington, DC 20426
4. Creditors Subject to Surface Transportation Board	Office of Proceedings, Surface Transportation Board Department of Transportation 395 E Street S.W. Washington, DC 20423
5. Creditors Subject to 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, SW, 8th Floor Washington, DC 20549
7. Brokers and Dealers	Securities and Exchange Commission 100 F St NE 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	FTC Regional Office for region in which the creditor operates or Federal Trade Commission: Consumer Response Center – FCRA Washington, DC 20580 (877) 382-4357

FCRA REQUIREMENTS

Federal Fair Credit Reporting Act (as amended by the Consumer Credit Reporting Act of 1996)

Although the FCRA primarily regulates the operations of consumer 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 Disclosure by Officers or Employees
- 621 Administrative Enforcement
- 623 Responsibilities of Furnishers of Information to Consumer Reporting Agencies
- 628 Disposal of Records

Each of these sections is of direct consequence to users who obtain reports on consumers.

As directed by the law, credit reports may be issued only if they are to be used for extending credit, review or collection of an account, employment purposes, underwriting insurance or in connection with some other legitimate business transaction such as in investment, partnership, etc. It is imperative that you identify each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact your usage of reports for employment purposes.

Data Facts, Inc. 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 statutes and regulation of the states in which you operate.