R-17-106

RESOLUTION NO. _____

A RESOLUTION AUTHORIZING EXECUTION OF A CONTRACT WITH ONLINE INFORMATION SERVICES, INC. FOR CREDIT SCORING SERVICES; AND FOR OTHER PURPOSES.

WHEREAS, the North Little Rock Electric Department ("NLRED") desires to accurately assess consumer credit risk by utilizing a soft credit check with a third-party vendor who is accustomed to the public utility business model; and

WHEREAS, the City issued requests for proposals for credit scoring services and determined the response of ONLINE Information Services, Inc. ("ONLINE") to be most favorable to the City and NLRED customers; and

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF NORTH LITTLE ROCK, ARKANSAS:

SECTION 1: That the General Manager of the North Little Rock Electric Department is hereby authorized to execute a contract with ONLINE Information Services, Inc. for credit scoring services that is substantially similar in form and content as the agreement attached hereto as Exhibit "A".

SECTION 2: That the funding for this resolution shall be substantially derived from user fees and included in the operational budget of the North Little Rock Electric Department.

SECTION 3: That this Resolution shall be in full force and effect from and after its passage and approval.

PASSED:

_____

APPROVED:

_____
Mayor Joe A. Smith

SPONSOR:

_____
Mayor Joe A. Smith

ATTEST:

_____
Diane Whitbey, City Clerk

APPROVED AS TO FORM:

_____
C. Jason Carter, City Attorney

PREPARED BY THE OFFICE OF THE CITY ATTORNEY

FILED 11:33 A.M. _____ P.M.
By J. Carter
DATE 6/20/17
Diane Whitbey, City Clerk and Collector
North Little Rock, Arkansas
RECEIVED BY T. McGraw

EXHIBIT
tabbies "A"

ON LINE
UTILITY EXCHANGE

SUBSCRIBER SERVICE AGREEMENT

This Subscriber Service Agreement ("Agreement") is entered into by **ONLINE Information Services, Inc.,** hereafter referred to as "ONLINE", a North Carolina corporation, d/b/a the ONLINE Utility Exchange and **City of North Little Rock** hereafter referred to as "Subscriber", a **Arkansas** corporation as of Thursday, June 01, 2017.

ONLINE and Subscriber agree as follows:

1. **Services.** Through the ONLINE Utility Exchange, ONLINE will furnish Services to Subscriber involving the supply of business and consumer information, consumer reports, credit worthiness scores, fraud detection, information pertaining to unpaid utility bills and other Services that ONLINE may, from time to time, make available to Subscriber ("Services"). Any mention of rights or obligations to ONLINE within this Agreement shall also apply to Experian, Trans Union, Equifax, Core Logic, LexisNexis, Background Data, and Rapid Courts ("Data Providers").

2. **Charges to Subscriber.**
   - **A.** Subscriber agrees to pay ONLINE for all charges for each Subscriber inquiry, including "no record found", submitted to ONLINE as outlined in SCHEDULE A "ONLINE Charges to Subscriber."
   - **B.** Bureau/Jurisdiction Surcharges and Fees. Subscriber acknowledges that Data Providers may impose additional surcharges for access to files that are affiliate owned or that reside in certain States or Counties. Additionally certain jurisdictions charge court fees for accessing public record information. Examples of these charges include Equifax Affiliate owned files, California Privacy Act Surcharges, and Alaska and Colorado State surcharges, and County Court fees. In the event that a file/report is accessed which has such a surcharge or fee ONLINE will pass that Surcharge/Fee along to the Subscriber.
   - **C.** Subscriber acknowledges that the pricing in Schedule A is based upon volume representations made by Subscriber during the negotiation of this Agreement. In the event that Subscriber fails to meet these volume expectations, ONLINE reserves the right to adjust its charges to accurately reflect the volume used by Subscriber.
   - **D.** Subscriber agrees that ONLINE aggregates data from third party sources and from time to time the cost to ONLINE to provide the Services may increase. ONLINE reserves the right to adjust Subscriber's pricing to reflect any such change with a 30 day notice to Subscriber prior to the change becoming effective.
   - **E.** Subscriber agrees that on each annual contract renewal the per inquiry price will increase by 2.5% of the then current price being paid by the Subscriber. This new per inquiry price will be reflected on the first invoice after the contract renewal with no additional notice to Subscriber.
   - **F.** Subscriber will be solely responsible for all federal, state and local taxes levied or assessed in connection with ONLINE's performance of the Services, other than income taxes assessed with respect to ONLINE's taxable net income, for which income taxes ONLINE will be solely responsible.

3. **Invoicing/Billing.**
   - **A.** Subscriber agrees that the pricing in Schedule A is based on Subscriber setting up and paying their monthly invoice via an automated payment method, either credit card or ACH.
   - **B.** All billing is processed monthly between the 1st and the 5th for the previous month's Services.
   - **C.** ONLINE will process the automated payment and deliver to Subscriber an invoice marked "Paid In Full".
   - **D.** All invoices will be delivered via electronic mail to the email addresses designated by Subscriber.
   - **E.** Subscriber agrees that, if their automated payment method is declined, ONLINE may charge a Non-Sufficient Funds fee, not to exceed $25.00.
   - **F.** A service charge of 2% of the unpaid balance will be charged on all accounts not paid by the 1st day of the month following the invoice date.
   - **G.** Services will be immediately terminated when account reaches 60 days past due. Services will not be reinstated until the full outstanding balance is paid in full and a valid automated payment method is setup with ONLINE.
   - **H.** If account remains unpaid for 90 days the account will be referred to collections and/or legal proceedings initiated. Subscriber agrees to pay ONLINE's cost and expenses, including reasonable attorney fees, to recover any unpaid balance owed by Subscriber.

4. **Subscriber Use.**
   - **A.** Subscriber hereby certifies and warrants that it will request and use consumer information received from ONLINE solely in connection with credit transactions involving the consumer as to whom such information is sought, or for other "permissible purposes" as defined by the Fair Credit Reporting Act, 15 U.S.C. Section 1681 *et seq.* (together with any successor or replacement statutory provisions, "FCRA")
   - **B.** Subscriber certifies that Subscriber shall use the Services:
     - i. Solely for Subscriber's certified permissible uses;
     - ii. Solely for Subscriber's exclusive one-time use.
   - **C.** Subscriber hereby certifies and warrants that it will request and use the fraud prevention portion of the service in compliance with a "permitted purpose" under the Gramm Leach Bliley Act, specifically fraud prevention and detection. Subscriber hereby certifies and warrants that it understands all obligations under the Gramm Leach Bliley Act.
   - **D.** As many ONLINE Services contain information from the Social Security Administration's Death Master File ("DMF"), Subscriber acknowledges its obligation to restrict Subscriber's use of deceased flags or other indicia within ONLINE's Services to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with Subscriber's 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. Subscriber certifies it will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within ONLINE's Services.
   - **E.** As many ONLINE Services contain information from the Social Security Administration's Death Master File ("DMF"), Subscriber acknowledges its obligations as outlined in Exhibit F, "Death Master File Access Requirements".
   - **F.** Subscriber maybe given access to information from state departments of motor vehicles. Subscriber hereby certifies and warrants that it will request and use the provided information only for an approved permissible purpose under the Drivers Privacy Protection Act, specifically fraud prevention and/or to affect collection of a debt.
   - **G.** If Subscriber obtains Social Security Numbers or Driver's License Numbers (SSNs) through the Services, Subscriber certifies it will not use the SSNs for any purpose other than, fraud prevention and/or to affect collection of a debt.
   - **H.** All such information shall be maintained by Subscriber in strict confidence and disclosed only to employees whose duties reasonably relate to the legitimate business purposes for which the information is requested, and Subscriber will not disclose, sell or otherwise distribute to third parties any information received hereunder, except as otherwise required by law; provided, however, that if Subscriber has purchased a consumer report from ONLINE in connection with a consumer's application for credit, and the consumer makes a timely request of Subscriber, Subscriber may share the contents of that report with the consumer as long as it does so without charge.
   - **I.** Subscriber acknowledges that it has received and reviewed a copy of the "Credit Scoring Services." (See Exhibit "A".)
   - **J.** Subscriber shall request consumer reports from ONLINE by electronic means. Each request will contain sufficient identifying information concerning the consumer about who the consumer report is requested to enable ONLINE to deliver the consumer report.
   - **K.** ONLINE reserves the right to modify the standard inquiry format to be used by Subscriber and Subscriber agrees to abide by such modifications.
   - **L.** Subscriber hereby certifies that it will properly dispose of any customer information obtained from the use of the Services to include the destruction or erasure of electronic media, the burning, pulverizing, or shredding of papers containing the customer information so that the information cannot practicably be read or reconstructed.
   - **M.** Subscriber may elect to receive Credit, Criminal, DMV and other consumer Information for the purpose of evaluating a potential or current employee's background. Information received by Subscriber may include data from Equifax, Experian, Trans Union, or other Data Providers. If Subscriber elects to receive Employment Reports Subscriber acknowledges the following:
     - i. Subscriber shall request consumer report for employment purposes pursuant to procedures prescribed by ONLINE from time to time only when it is considering the individual inquired upon for employment, promotion, reassignment, or retention as an employee, and for no other purpose. Subscriber shall comply with any federal and state laws which may restrict or ban the use of consumer reports for employment purposes.
     - ii. A clear and conspicuous disclosure has been made in writing to the consumer at any time before the report is procured or caused to be procured, in a document that consists solely of the disclosure, that a consumer report (to include credit and criminal) may be obtained for employment purposes.
     - iii. The consumer has authorized in writing the procurement of the Employment Report by the subscriber.
     - iv. To include on their application for employment a signed authorization and release section giving permission for the Subscriber to pull an Employment Report to investigate the applicant.
     - v. To keep documentation on the applicant (Signed Employment Application, Copy of Employment Report) on file in their office for 5 years.
     - vi. Subscriber agrees that Employment Reports will be the only consumer reporting products pulled to screen employment applicants.
     - vii. Subscriber warrants it will use the consumer report for employment purposes only for a one time use, and shall hold the report in strict confidence, and not disclose it to any third parties that are not involved in the employment decision.
     - viii. Subscriber acknowledges that before taking any adverse action based in whole or in part on the Employment Report (if an offer is not extended to applicant based on information contained within the Employment Report), a copy of the report which contains the applicant's rights under the Fair Credit Reporting Act must be given to the applicant.
     - ix. The information from ONLINE's Employment Reports will not be used in violation of any applicable federal or state equal employment opportunity law or other regulation. Subscriber hereby acknowledges receipt of "Notice to Users of Consumer Reports: Obligations of Users Under FCRA". (See Exhibit "B".)

N. California and Vermont Users

i. Subscriber agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act. Subscriber certifies that it _____ IS or _____ IS NOT a "Retail Seller", as defined in Section 1802.3 of the California Civil Code, doing business in California and issues credit to consumers who appear in person that it will instruct its employees and agents to inspect a photo identification of the consumer at the time the application is submitted in person. This paragraph does not apply to an application for credit submitted by mail.

ii. Subscriber acknowledges that it has received and reviewed a copy of the "Requirements for California and Vermont Users." (See Exhibit "C")

K. Subscriber further agrees that it will be solely responsible to ensure and require that each of its users meets and complies with applicable federal, state and local laws, rules, and regulations relating to its use of the Services and to the provision to ONLINE of Subscriber's Records. Relevant laws include but are not limited to:

i. Establishing reasonable procedures to insure that its employees will not request Data Services relating to themselves, their families, friends, or request consumer information on other persons other than as permitted by the FCRA, ONLINE, and this Agreement.

ii. Where adverse action is taken against a consumer that is based in whole or in part on the information contained in a consumer report provided by ONLINE, consistent with the responsibilities under the Fair Credit Reporting Act, Subscriber shall notify the Consumer to direct consumer inquiries to the CRA that provided the report and contained on the adverse action notice for such report.

L. **Record Retention.** *The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 60 months. In keeping with the ECOA, the credit reporting agency requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 60 months. When conducting an investigation, particularly following a breach or a consumer complaint that your company impermissibly accessed their credit report, the credit reporting agency will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract. "Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $2,500 per violation."*

5. ONLINE Use.

A. The ONLINE Utility Exchange acknowledges its qualification as a specialty consumer reporting agency according to the Fair Credit Reporting Act: § 603 Definitions; rules of construction [15 U.S.C. § 1681a]: "(f) The term "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."

B. As a consumer reporting agency, ONLINE may only use Subscriber's records for purposes consistent with applicable federal, state, and local laws, rules, and regulations' in the identification of credit risk and/or to recover unpaid accounts.

C. ONLINE shall not sell or furnish to any third party a list of consumers' names and addresses identified as a current or previous customer of Subscriber, nor will ONLINE extract directly from or otherwise identify on any third party's list a list of Subscriber's customers identified as a customer list of Subscriber. In no event shall ONLINE distribute a list of Subscriber's current or previous customers outside of the uses defined in this Agreement.

D. ONLINE shall use commercially reasonable efforts to promptly and accurately process and incorporate into its database any record updates or consumer dispute verifications furnished to it by Subscriber, in accordance with the requirements of the FCRA or other applicable state or federal law. In the event that ONLINE deems any record updates or verification response of Subscriber to be incomplete, internally inconsistent, or otherwise inaccurate, ONLINE, in its sole discretion, may revise the item of information to conform with information supplied by the consumer, reject the record update or verification response and delete the information from its database, or make any other revisions that it deems necessary or appropriate.

6. FCRA Requirements

A. Although the FCRA primarily regulates the operations of consumer reporting agencies, it also affects Subscriber as a user of information. ONLINE has included a copy of the FCRA with Subscriber's membership kit and it is posted at http://www.ftc.gov/us/statutes/fcradoc.pdf. ONLINE suggests that Subscriber and Subscriber's employees become familiar with the following sections in particular:

§ 604. Permissible Purposes of Reports
§ 607. Compliance Procedures
§ 615. Requirement on users of consumer reports
§ 616. Civil liability for willful noncompliance
§ 617. Civil liability for negligent noncompliance
§ 619. Obtaining information under false pretenses
§ 621. Administrative Enforcement
§ 623. Responsibilities of Furnishers of Information to Consumer Reporting Agencies
§ 628. Disposal of Records

B. Each of these sections is of direct consequence to users who obtain reports on consumers. See Exhibit "B" for "Notice to Users of Consumer Reports: Obligations of Users Under the FCRA".

C. As directed by law, consumer 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 Subscriber identifies each request for a report to be used for employment purposes when such report is ordered. Additional state laws may also impact Subscriber's usage of reports for employment purposes.

D. ONLINE strongly endorses the letter and spirit of the Federal Fair Credit Reporting Act. ONLINE believes 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.

E. 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, ONLINE expects that Subscriber will comply with all relevant federal statutes and the statutes and regulations of the states in which Subscriber operates. 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.

7. **Conditions.** Subscriber recognizes that ONLINE's Services require open sharing of information between Subscribers.

A. Subscriber agrees to furnish to ONLINE, information from its records about its current and/or previous customers with whom it has established accounts. Such information will be furnished and updated no less frequently than at monthly intervals, unless otherwise agreed in writing. Subscriber hereby certifies that all information furnished to ONLINE shall be complete and accurate. Subscriber therefore has the option to, make a list of all current customers, including the service address, telephone number, place of employment and employment telephone number (hereafter referred to as Utility Exchange Data), as well as a list of all current or previous customers who have unpaid utility bills more than 30 days old (hereafter referred to as Utility Exchange Data). Subscriber agrees that each account will be accompanied by the Social Security Number of the guarantor of the bill and, in the case of married parties or joint responsibility by more than one guarantor, the Social Security Number of each party who is responsible for payment of the bill.

B. Subscriber agrees they are a Data Furnisher as defined by the Fair Credit Reporting Act and will comply with the "Obligations of Furnishers" as attached in Exhibit "D".

C. Subscriber agrees to notify ONLINE within 30 days of receipt of payment on any account which is part of ONLINE's Utility Exchange Data.

D. Subscriber shall respond to any consumer disputes initiated by consumer within five (5) working days from receipt of dispute. Subscriber shall re-verify disputed information through either voice communication, electronic mail, or through other means as mutually agreed in writing. Subscriber certifies that all information supplied by it on any automated or manual basis in response to a consumer dispute verification request sent to it by ONLINE shall be complete and accurate. If in response to a consumer dispute verification request received from ONLINE, Subscriber desires to change any information relating to an account it has previously reported, Subscriber shall update the account information on both the verification response and in its own internal records to conform to such change. Subsequent customer record updates provided by Subscriber shall reflect such change.

E. In the event that Subscriber fails to contribute Utility Exchange Data to the ONLINE Utility Exchange within 180 days of the effective date of this Agreement, ONLINE shall consider the Subscriber to be a Non-Data Contributing Subscriber and shall impose a Non Data Contributor Surcharge of an additional $.25 per inquiry.

8. **Term and Termination.**

A. This Agreement is for a period of 12 months from the effective date and will automatically renew annually unless terminated by either party in writing at least 30 days prior to the then current expiration date.

B. Notwithstanding the foregoing, if Subscriber is delinquent in the payment of charges, violates the FCRA or other applicable law or violates a material term of this Agreement, ONLINE may, at its election, discontinue providing the Services to Subscriber and terminate this Agreement immediately by written notice to the Subscriber.

C. Notwithstanding anything to the contrary in this Agreement, if the continued provision of the Services or any affected component thereof becomes impossible, impractical, or undesirable due to a change in applicable federal, state, or local laws or regulations, as determined by ONLINE in its reasonable judgment, or due to circumstances imposed by ONLINE's third party vendors or Data Providers, ONLINE may either (a) cease to provide the Services or any affected component thereof within, or pertaining to persons residing within, the affected jurisdiction, or (b) establish new prices which apply to ONLINE's Services or any affected component thereof when provided or delivered within, or pertaining to persons residing within, the affected jurisdiction, which prices will be reasonably calculated to cover the costs incurred by ONLINE in complying with the applicable laws or regulations or circumstances imposed by third party Data Providers and will become effective on the date specified in such notice unless Subscriber objects in writing, in which case ONLINE may exercise its rights under clause (a) above. ONLINE will attempt to provide written notice of its actions as far in advance of the effective date as reasonably possible under the circumstances.

D. **No Damages or Indemnification for Termination.** Neither party shall be liable to the other party for any costs or damages of any kind, including direct, special, exemplary, punitive, indirect, incidental or consequential damages, or for indemnification, solely on account of the lawful termination of this Agreement, even if informed of the possibility of such damages.

9. **Warranties.**
   A. **ONLINE Utility Exchange.** Subject to Section 18 "Excusable Delays" hereof, ONLINE warrants to Subscriber that ONLINE will use commercially reasonable efforts to deliver the Services promptly. Subscriber acknowledges that the Services involve information provided to ONLINE by fallible human sources and that for the fee charged for the Services, ONLINE cannot and will not be an insurer or guarantor of the accuracy or reliability of the Services, data contained in its database, or data provided with the Services. THE WARRANTY IN THE FIRST SENTENCE OF THIS PARAGRAPH IS THE ONLY WARRANTY ONLINE HAS GIVEN SUBSCRIBER WITH RESPECT TO THE SERVICES AND SUCH WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ONLINE MIGHT HAVE GIVEN SUBSCRIBER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE AND WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
   B. **Credit Scoring.** ONLINE's Credit Scoring Vendors warrant that these Credit Scoring Models are empirically derived and demonstrably and statistically sound and that to the extent the population to which the Credit Scoring Model is applied is similar to the population sample on which the Credit Scoring Model was developed, the Credit Scoring Model score may be relied upon by Subscriber to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to Subscriber. ONLINE's Credit Scoring Vendors further warrant that so long as they provide the Credit Scoring Model, they 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 ONLINE'S CREDIT SCORING VENDORS HAVE GIVEN SUBSCRIBER WITH RESPECT TO THEIR CREDIT SCORING MODEL AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, ONLINE'S CREDIT SCORING VENDORS MIGHT HAVE GIVEN SUBSCRIBER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Subscriber's rights under the foregoing Warranty are expressly conditioned upon Subscriber's periodic revalidation of the Credit Scoring Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 *et seq.*). ONLINE shall not be deemed to have made (nor shall ONLINE be liable or responsible for in any respect for the application or enforcement of) any warranty set forth in this Section 9.B.
   C. **Criminal Reports.** With respect to criminal reports available from ONLINE, neither ONLINE nor any division thereof nor any of its employees or officers or directors, makes any warranty, expressed or implied, including warranties of merchantability and fitness for a particular purpose or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process disclosed, or represents that its use would not infringe on privately owned rights. Subscriber hereby acknowledges that ONLINE does not create or maintain these records or information, and that ONLINE relies on third party sources including, but not limited to, data providers, state departments, state repositories, correctional institutions, the courts and other information sources. Subscriber understands ONLINE is not responsible for the content or accuracy of such records or information and ONLINE suggests that these searches should only be used as a preliminary inquiry. The records obtained from these searches must be used in complete compliance with the Fair Credit Reporting Act, Fair Housing Laws, and any other state or federal laws governing the use of public records. Although every effort is made to assure the accuracy of the information contained in these reports the Subscriber releases, indemnifies and holds harmless ONLINE to the fullest extent allowed by law with respect to Subscriber's receipt and/or use for any reason, of any information provided by ONLINE. Subscriber acknowledges that data entry errors or incomplete records may result in the return of incorrect results. ONLINE cannot offer legal advice on how to use the information contained in these reports and is not responsible for any action taken by Subscriber based on this information.

10. **Limitation of Liability.** Subscriber acknowledges that ONLINE maintains a database, updated on a periodic basis, from which Subscriber solicits information, and that ONLINE does not undertake a separate investigation for each inquiry or request for Services made by Subscriber. Subscriber also acknowledges that ONLINE provides Subscriber access to national consumer reporting agencies and various products and services available to Subscriber from these repositories through ONLINE. With regard to limitation of liability, any mention of ONLINE shall also apply to Experian, Trans Union, Equifax, LexisNexis, Core Logic, Rapid Courts, and Background Data (Data Providers). Subscriber also acknowledges that the prices ONLINE charges Subscriber for the Services are based upon ONLINE's expectation that the risk of any loss or injury that may be incurred by use of the Services will be borne by Subscriber and not ONLINE. Subscriber therefore agrees that it is responsible for determining that the Services are in accordance with ONLINE's obligations under this Agreement. If Subscriber reasonably determines that the Services do not meet ONLINE's obligations under this Agreement, Subscriber shall so notify ONLINE in writing within ten (10) days after receipt of the Services in question. Subscriber's failure to so notify ONLINE shall mean that Subscriber accepts the Services as is, and ONLINE shall have no liability whatsoever for the Services. Unless ONLINE disputes Subscriber's claim, ONLINE shall, at its option, either re-perform the Services in question or issue Subscriber a credit for the amount Subscriber paid for the nonconforming Services. This re-performance or credit constitutes Subscriber's sole remedy and ONLINE's maximum liability for any breach of this Agreement by ONLINE. If, notwithstanding the above, liability is imposed on ONLINE, then Subscriber agrees that ONLINE's total liability for any or all of Subscriber's losses or injuries from ONLINE's acts or omissions under this Agreement, regardless of the nature of the legal or equitable right claimed to have been violated, shall not exceed the amount paid by Subscriber to ONLINE under this Agreement during the six month period preceding the alleged breach by ONLINE of this Agreement. Subscriber covenants that it will not sue ONLINE for any amount greater than permitted by this Agreement. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL ONLINE HAVE ANY OBLIGATION OR LIABILITY TO SUBSCRIBER HEREUNDER FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL OR SPECIAL DAMAGES INCURRED BY THE SUBSCRIBER (INCLUDING DAMAGES FOR LOST BUSINESS, LOST PROFITS OR DAMAGES TO BUSINESS REPUTATION), REGARDLESS OF HOW SUCH DAMAGES ARISE AND REGARDLESS OF WHETHER OR NOT THE SUBSCRIBER WAS ADVISED SUCH DAMAGES MIGHT ARISE.

11. **Hold Harmless.** Subscriber agrees that some of the information it will have access to maybe provided by third parties to include Equifax, Experian, Trans Union, LexisNexis, Core Logic, Rapid Courts, and Background Data (Data Providers). Without limitation of its obligations of indemnification to ONLINE under this Agreement or under applicable law, Subscriber shall indemnify save and hold ONLINE's Suppliers, their officers, directors, employees, agents, contractors and subcontractors harmless for any and all injuries, damages, claims, costs and expenses arising out of Subscriber's use of the Services.

12. **Indemnification.** Subscriber shall indemnify, defend and hold ONLINE and ONLINE Utility Exchange harmless from and against any and all claims, losses, damages, costs and expenses, including reasonable attorney fees, which may be asserted against or incurred by ONLINE or ONLINE Utility Exchange, based upon the use by Subscriber of the Services or other information furnished by ONLINE for purposes not permitted by law. Subscriber shall be liable for its own acts of negligence, and Subscriber shall hold ONLINE harmless and indemnify ONLINE for any claims, damages, loss, cost, expense or liability (including reasonable attorney's fees) incurred by ONLINE as a result of Subscriber's negligence in the furnishing of data to ONLINE, Subscriber's failure to perform any of its obligations described in this Agreement or any other breach by Subscriber of its obligations under this Agreement, or Subscriber's failure to comply with the FCRA.

13. **Access Security.** Subscriber acknowledges that it has received and reviewed a copy of the "Access Security Requirements." (See Attachment E.)

    A. **Subscriber will notify ONLINE immediately as any approved User leaves or is terminated so that the User can be deactivated from the ONLINE system.**

14. **Intellectual Property.** Subscriber acknowledges that ONLINE has expended substantial time, effort and funds to create and deliver the Services and compile its consumer reporting database. The Services and the data in ONLINE's Consumer Reporting databases are and will continue to be ONLINE's exclusive property. Nothing contained in this Agreement shall be deemed to convey to Subscriber or to any other party any right, title or interest, including any patent, copyright or other proprietary right, in or to the Services or data in ONLINE's Consumer Reporting database. Subscriber will not use or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names, or any other of ONLINE's or its affiliates' proprietary designations, whether registered or unregistered, without ONLINE's prior written consent. Under no circumstances will Subscriber attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by ONLINE, it's Data Providers, or its credit scoring vendors.

15. **Non-Solicit Clause.** During the term of this Agreement and for a period of 1 year subsequent to the termination of this Agreement, neither party shall: (i) solicit, or encourage any organization directly or indirectly controlled by its management, Board, or shareholders, to solicit, any employee of the opposing party or any of its subsidiaries to leave the employ of the opposing party or any of its subsidiaries, (ii) solicit for employment, hire or engage as an independent contractor, or permit any organization directly or indirectly controlled by its management, Board, or shareholders, to solicit for employment, hire or engage as an independent contractor, any person who was employed by the opposing party or any of its subsidiaries at any time during the term of the Employee's employment with the other party or any of its subsidiaries; provided, that this clause shall not apply to any individual whose employment with the opposing party or any of its subsidiaries has been terminated for a period of one year or longer.

16. **Waiver.** Either party may at any time waive compliance by the other with any covenant or condition contained in this Agreement, but only by written instrument signed by the party waiving such compliance. No such waiver, however, shall be deemed to constitute the waiver of any such covenant or condition in any other circumstance or the waiver of any other covenant or condition.

17. **Successors and Assigns.** This Agreement will be binding upon and will inure to the benefit of the parties hereto and their respective heirs, representatives, successors and permitted assignees. This Agreement may not be assigned, transferred, shared or divided in whole or in part by Subscriber without prior written consent; such consent shall not be unreasonably withheld.

18. **Audit Rights.** Subscriber understands that ONLINE and each of ONLINE's Data Providers require the right to audit usage by Subscriber for compliance with the requirements of the Federal Fair Credit Reporting Act. Subscriber herein agrees to cooperate fully with any compliance audit by ONLINE or ONLINE's Data Providers and to provide ONLINE any required documentation or other information necessary for such an audit in a timely and reasonable manner.

19. **Excusable Delays.** Neither party shall be liable for any delay or failure in its performance under this Agreement (other than for payment obligations hereunder) if and to the extent that such delay or failure is caused by events beyond the reasonable control of the party including, without limitation, acts of God or public enemies, labor disputes, equipment malfunctions, computer downtime, software defects, material or component shortages, supplier failures, embargoes, rationing, acts of local, state or national governments or public agencies, utility or communication failures or delays, fire, earthquakes, flood, epidemics, riots and strikes.

20. **Dispute Resolution.** With the exception of any action taken under paragraphs 1 and 4 or any alleged violation of paragraph 9, 10 and 16 of this Agreement, the parties will resolve any dispute arising out of or relating to this Agreement in a binding arbitration conducted under the auspices of the American Arbitration Association. Disputes arising out of or resulting from actions taken under paragraphs 1, 4 or 9, 10 and 16 may be resolved informally by the parties through the courts.

21. **Site Inspection.** Subscriber agrees to an inspection of its premises by an independent Third Party Inspection Agency. The inspection is to be completed, in a timely manner, before any Services will be set up with our company. Subscriber's Application Fee will be applied to cover the cost of the Inspection Fee. Subscriber also agrees that this fee is non-refundable.

22. **Continuance of Business.** In the event that Subscriber's business is sold or relocates to a different location, it is the Subscriber's obligation to notify ONLINE, in writing, of these changes, within 72 business hours of the effective date of the transaction or the relocation.

23. **Notifications.** Subscriber and ONLINE agree that any notifications to the other as it pertains to this Agreement shall be sent to the following contacts.

ONLINE Information Services, Inc.
J.W. Blair, President
P.O. Box 1489
Winterville, NC 28590
Fax: (800) 838-9830

City of North Little Rock
Subscriber Company Name

Subscriber Contact Name, Title
P.O. Box 936
Subscriber Mailing Address
North Little Rock, Arkansas 72115
Subscriber City, State, Zip
Fax:_____

24. **Severability.** This Agreement shall be deemed to be severable and, if any provision is determined to be void or unenforceable, then that provision will be deemed severed and the remainder of the Agreement will remain in effect.

25. **Contract in Entirety; Law.** This Agreement sets forth the entire understanding and agreement between ONLINE and Subscriber concerning the Services, and supersedes any prior or contemporaneous oral or written agreements or representations. It may be modified only by a written amendment executed by both parties. This Agreement shall be interpreted in accordance with the laws of the State of North Carolina.

26. **Effective Date.** This Agreement is effective beginning June 1, 2017.

[Signature Page to Follow.]

IN WITNESS WHEREOF, the parties' authorized representatives have executed this Agreement on the date indicated below.

Subscriber hereby certifies to have read and understand the **"FCRA Requirements"** notice and **"Access Security Requirements"** and will take all reasonable measures to enforce them within Subscribers facility. Subscriber certifies that a permissible purpose exists to use all Services accessed from ONLINE in accordance with the Fair Credit Reporting Act and the applicable service agreement. Subscriber also certifies that information obtained from ONLINE will be used for the purpose(s) listed below and no other. Subscriber will not resell the report to any third party.

PERMISSIBLE PURPOSE/APPROPRIATE USE: Describe the **specific purpose(s)** (a clear definition) for which **ONLINE** Services and consumer data will be used. (An answer like "Checking Credit" is not a permissible purpose.):

_____

_____

_____

Subscriber: _____

Signature: _____

Print Name: _____

Title: _____

Email: _____

Date: _____

Federal Tax ID: _____

Address of Principal Business Office:

120 Main Street

North Little Rock, Arkansas 72114

Mailing Address (If Different):

P.O. Box 936

North Little Rock, Arkansas 72115

ONLINE Information Services, Inc.
dba/ ONLINE Utility Exchange

By: _____

Christoph Turner
Sales Manager

Date: _____

Address: PO Box 1489
Winterville, NC 28590
www.ONLINEUtilityExchange.com

Telephone: (866) 630-6400
Fax: (800) 838-9830

SCHEDULE A
ONLINE Charges to Subscriber

Please denote beside each product what level user should have access. Please note that if Administrator (Admin) level is assigned, Supervisors (Super) and Users (User) will not have access to those products. And likewise if a Supervisor level is assigned Users will not have access to those products. If you desire for all individuals at your organization to have access to a product please set the Access Level for that product to User.

			User/Super/Admin Access Level
ONLINE Utility Exchange Pricing:			
ONLINE Utility Exchange Report:	$2.50	Per Report	User
Monthly Access Fee	$Waived	Per Month	
Adverse Action/Score Disclosure Letter Service (Y / N)	$1.10	Per Letter Mailed by OIS	
OTHER SERVICES OFFERED:			
Business Report Pricing:			
Business Intelliscore Report	$17.25	Per Report	
Business Profile Report	$33.25	Per Report	
Business Profile w/ Intelliscore Report	$37.50	Per Report	
Employment Screening Reports Pricing:			
Employment Credit Report	$15.00	Per Report	
Employment Criminal Report Pricing:			
National Criminal Search	$20.00	Per Report	
Statewide Instant Search	$12.00	Per Report	
County Search (Non-Instant)	$20.00	Per Report Plus Court Fees	
Non-Instant State Search	$17.00	Per Report	
National Sex Offender Only Search	$10.00	Per Report	
Additional Report Pricing:			
Full Credit File with Score	$ 4.00	Per Report	
ONLINE People Search	$ 0.35	Per Search	
Collection Report	$ 4.00	Per Report	
Social Search	$ 1.80	Per Search	

OFFICE USE:

Cr Source: _____ CF_____
Ev Source: _____ CR_____EV_____

SCHEDULE A Continued
ONLINE Charges to Subscriber

State Department of Motor Vehicles Search for Employment Purposes

State	Report Options (If Any)	Turn Around Time	Price
Alabama		Same Day	$ 17.00
Alaska		Next Day	$ 12.00
Arizona	5 year Employment:	Same Day	$ 15.50
	5 year Employment:	Next Day	$ 13.50
Arkansas	Employment:	Same Day	$ 20.00
California		Same Day	$ 10.00
Colorado		Same Day	$ 10.00
Connecticut		Same Day	$ 25.00
Delaware		Same Day	$ 32.00
District of Columbia		Same Day	$ 20.00
Florida	3-year:	Same Day	$ 15.00
	7-year:	Same Day	$ 17.00
	Complete:	Same Day	$ 17.00
Georgia	3-year:	Same Day	$ 13.00
	7-year:	Same Day	$ 15.00
Hawaii		Next Day	$ 30.00
Idaho		Same Day	$ 16.00
Illinois		Same Day	$ 19.00
Indiana		Same Day	$ 15.00
Iowa		Same Day	$ 16.00
Kansas		Same Day	$ 16.00
Kentucky		Same Day	$ 13.00
Louisiana		Same Day	$ 23.00
Maine		Same Day	$ 14.00
Maryland		Same Day	$ 19.00
		Same Day	$ 15.00
Michigan		Same Day	$ 15.00
Continued			
Minnesota	CDL	Same Day	$ 12.00
	Database	Same Day	$ 11.50
Mississippi		Same Day	$ 21.00
Missouri		Next Day	$ 12.00
Montana		Same Day	$ 15.00
Nebraska		Same Day	$ 10.00
Nevada		Same Day	$ 15.00
New Hampshire		Same Day	$ 20.00
New Jersey		Same Day	$ 19.00

New Mexico		Same Day	$ 14.00
New York		Same Day	$ 14.00
North Carolina	3 year:	Same Day	$ 15.00
	7 Year:	Same Day	$ 17.00
North Dakota		Same Day	$ 10.00
Ohio		Same Day	$ 12.00
	Monthly Database	Same Day	$ 10.00
Oklahoma		Same Day	$ 35.00
Oregon	Employment:	Same Day	$ 16.50
Pennsylvania		Same Day	$ 18.00
Rhode Island		Same Day	$ 27.00
South Carolina	3 Year:	Same Day	$ 14.00
	10 Year:	Same Day	$ 15.00
South Dakota		Same Day	$ 12.00
Tennessee		Same Day	$ 14.00
	Monthly Database	Same Day	$ 10.00
Texas	5 year Employment:	Same Day	$ 15.00
Utah		Same Day	$ 16.00
Vermont		Same Day	$ 24.00
Virginia		Same Day	$ 14.00
Washington	5 Year Employment:	Same Day	$ 20.00
West Virginia		Same Day	$ 16.00
Wisconsin		Same Day	$ 14.00
Wyoming		Same Day	$ 12.00

*******Note: If Tax exempt, please provide certificate*******

Subscriber agrees to the above pricing schedule for reports pulled from ONLINE Information Services, Inc.

_____
(Subscriber's Name)

_____ _____
(Subscriber's Signature) (Date)

Exhibit "A"
Credit Scoring Services

Subscriber is a credit grantor that purchases Consumer Reports from ONLINE pursuant to the Agreement in connection with credit transactions involving the consumer subjects of such Consumer Reports. As an enhancement to the basic Consumer Report, ONLINE has offered Subscriber the opportunity to purchase one or more credit risk scores provided by Trans Union, Equifax, or Experian; including, but not limited to, Fair Isaac & Co. (FICO) and Vantage score models. Use of these scoring models may require additional addendums and be subject to additional terms of use.

Subscriber recognizes that all credit risk scores offered hereunder are statistical scores and may not be predictive as to any particular individual. No such score is intended to characterize any individual as to credit capability. Subscriber recognizes that factors other than credit risk scores should be considered in making a credit decision, including the Credit Report, the individual credit application, economic factors, and various other pertinent information. A statement of the factors that significantly contributed to the credit risk score may accompany the score. If so, such information may be disclosed to the consumer as the reason for taking adverse action, as required by Regulation B. However, the credit risk score itself is proprietary and may not be used as the reason for adverse action under Regulation B. In addition, under the Fair Credit Reporting Act, credit risk scores are not considered part of the consumer's file. Accordingly, Subscriber agrees only to disclose the actual credit risk score to the consumer as required by law and when accompanied by the corresponding reason codes.

SUBSCRIBER HAS MADE ITS OWN ANALYSIS OF THE CREDIT RISK SCORE OR SCORES SELECTED BY SUBSCRIBER, INCLUDING THE RELIABILITY OF USING SUCH SCORES IN CONNECTION WITH SUBSCRIBER'S CREDIT DECISION. ONLINE AND ITS AGENTS SHALL NOT BE LIABLE FOR ANY LOSS, COSTS, DAMAGES, OR EXPENSE INCURRED BY SUBSCRIBER RESULTING FROM SUBSCRIBER'S USE OF CREDIT RISK SCORES, OR THE INACCURACY THEREOF. IN NO EVENT SHALL ONLINE NOR ITS AGENTS BE LIABLE TO SUBSCRIBER FOR ANY INCIDENTAL, INDIRECT, PUNITIVE, OR CONSEQUENTIAL DAMAGES FOR A CLAIM BY SUBSCRIBER RESULTING FROM SUBSCRIBER'S USE OF ANY CREDIT RISK SCORE. THE TOTAL AGGREGATE LIABILITY OF ONLINE AND ITS AGENTS FOR A CLAIM BY SUBSCRIBER RELATED TO SUBSCRIBER'S USE OF ANY CREDIT RISK SCORE SHALL NOT EXCEED THE SURCHARGE PAID BY SUBSCRIBER FOR THE CREDIT RISK SCORE TO WHICH SUCH CLAIM RELATES.

Subscriber certifies that in using the FICO/VANTAGE Credit Scoring Models that:

A. Subscriber will only use the permissible purpose as outlined within ONLINE's Subscriber Service Agreement (hereinafter referred to as "Agreement") and the Application for Service in accordance with the FCRA to obtain the information derived from the Fair Isaac and Company Scoring Model (hereinafter referred to as "FICO") or the Vantage Scoring Model.
B. Subscriber will limit Subscriber's use of the scores and reason codes solely to use in Subscriber's own business with no right to transfer or otherwise sell, license, sublicense or distribute said scores or reason codes to third parties.
C. Subscriber will maintain internal procedures to minimize the risk of unauthorized disclosure and agree that such scores and reason codes will be held in strict confidence and disclosed only to those employees with a "need to know" and to no other person.
D. Notwithstanding any contrary provision of the Agreement, Subscriber may disclose the scores provided to Subscriber under the Agreement to the consumer, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only as required by law.
E. Subscriber will comply with all applicable laws and regulations in using the scores and reason codes purchased from ONLINE.
F. Subscriber or any of its employees, agents or subcontractors will not use any trademarks, service marks, logos, names, or any other proprietary designations, whether registered or unregistered, of the Data Providers or Fair, Isaac and Company, or their affiliates without such entity's prior written consent.
G. Subscriber will not in any manner, directly or indirectly attempt to discover or reverse engineer any confidential and proprietary criteria developed or used by the Data Providers/Fair, Isaac in performing the FICO/Vantage Scoring Model.
H. Subscriber will not use any of the scores provided for their own model development or model calibration.
I. Subscriber understands that Data Providers/FICO warrants that the FICO/Vantage Scoring Model are empirically derived and demonstrably and statistically sound and that to the extent the populations to which the FICO/Vantage Scoring Models are applied is similar to the population sample on which the FICO/Vantage Scoring Models were developed, the FICO/Vantage score may be relied upon by Subscriber to rank consumers in the order of the risk of unsatisfactory payment such consumers might present to Subscribers. FICO/Vantage further warrant that so long as FICO/Vantage provide the FICO/Vantage 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 DATA PROVIDERS, FICO, OR VANTAGE HAVE GIVEN SUBSCRIBER WITH RESPECT TO FICO/VANTAGE SCORING MODELS AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, DATA PROVIDERS, FICO, OR VANTAGE MIGHT HAVE GIVEN SUBSCRIBER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE. Subscriber's rights under the foregoing Warranty are expressly conditioned upon each respective Subscriber's periodic revalidation of the FICO/Vantage Scoring Model in compliance with the requirement of Regulation B as it may be amended from time to time (12 CFR Section 202 *et seq.*).
J. Subscriber agrees that the aggregate liability of the Data Providers/FICO to the Subscriber is equal to the lesser of the Fees paid by ONLINE to the Data Providers/FICO for the FICO/Vantage Scoring Models resold to the pertinent Subscriber during the six (6) month period immediately preceding the Subscriber's claim, or the fees paid by the pertinent Subscriber to ONLINE under the Agreement during said six (6) month period and excluding any liability of the Data Providers/FICO for incidental, indirect, special or consequential damages of any kind.

Initial

Exhibit "B"

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 EMPLOYEE INVESTIGATIONS
Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long 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. Disclosure and Certification Requirements

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

- Disclose the identity of the end-user to the source CRA.
- Identify to the source CRA each permissible purpose for which the report will be furnished to the end-user.
- Establish and follow reasonable procedures to ensure that reports are resold only for permissible purposes, including procedures to obtain:
  (1.) the 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
Section 603
15 U.S.C. 1681
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. 1681y

Exhibit "C"
Requirements for California and Vermont Users

California Users:

Provisions of the California Consumer Credit Reporting Agencies Act, as amended effective July 1, 1998, will impact the provision of consumer reports to Subscriber under the following circumstances: (a) if Subscriber is a "retail seller" (defined in part by California law as "a person engaged in the business of selling goods or services to retail buyers") and is selling to a "retail buyer" (defined as "a person who buys goods or obtains services from a retail seller in a retail installment sale and not principally for purpose of resale") and a consumer about whom Subscriber is inquiring is applying, (b) in person and (c) for credit. Under the foregoing circumstances, ONLINE, before delivering a Consumer Report to Subscriber, must match at least three (3) items of a consumer's identification within the file maintained by the Data Providers with the information provided to Data Provider's via ONLINE by Subscriber in connection with the in-person credit transaction. Compliance with this law further includes Subscriber's inspection of the photo identification of each consumer who applies for in-person credit, mailing extensions of credit to consumer responding to a mail solicitation at a specified address, taking special actions regarding a consumer's presentment of a police report regarding fraud, and acknowledging consumer demands for reinvestigations within certain time frames.

If Subscriber is a "retail seller," Subscriber certifies that it will instruct its employees to inspect a photo identification of the consumer at the time an application is submitted in person. If Subscriber is not currently, but subsequently becomes a "retail seller," Subscriber agrees to provide written notice to ONLINE prior to ordering Consumer Reports in connection with an in-person credit transaction, and agrees to comply with the requirements of the California law as outlined in this Attachment, and with the specific certifications set forth herein.

Subscriber certifies that, as a "retail seller," it will either (a) acquire a new Subscriber number for use in processing Consumer Report inquiries that result from in-person credit applications covered by California law, with the understanding that all inquiries using this new Subscriber number will require that Subscriber supply at least three items of identifying information form the applicant; or (b) contact ONLINE sales representative to ensure that Subscriber's existing Subscriber number is properly coded for these transactions.

Vermont Users:

Subscriber acknowledges that it subscribes to receive various information Services from ONLINE, Inc. in accordance with the Vermont Fair Credit Reporting Statute, 9 V.S.A. §2480e (1999), as amended (the "VFCRA") and the Federal Fair Credit Reporting Act, 15, U.S.C. 1681 et. Seq., as amended (the "FCRA") and its other state law counterparts. In connection with Subscriber's continued use of ONLINE Services in relation to Vermont consumers, Subscriber herby certifies as follows:

Vermont Certification. Subscriber certifies that it will comply with the applicable provisions under Vermont law. In particular, Subscriber certifies that it will order certain information relating to Vermont residents, that are Consumer Reports as defined by the VFCRA, only after Subscriber has received prior consumer consent in accordance with the VFCRA § 2480e and applicable Vermont Rules. Subscriber further certifies that the attached copy § 2480e of the Vermont Fair Credit Reporting Statute was received from ONLINE.

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 the 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 account, increasing the credit line on the account, for the purpose of taking collection action on the account, or for other legitimate purposes associated with the account; and
  (2) the use of credit information for the purpose of prescreening, as defined and permitted from time to time by the Federal Trade Commission.

Initial

VERMONT RULES
***** CURRENT THROUGH JUNE 1999 *****
AGENCY 06. OFFICE OF THE ATTORNEY GENERAL
SUB-AGENCY 031. 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 governmental benefit. If the consumer has applied for or requested credit, insurance, employment, housing or governmental 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 report 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 "D"

All furnishers of information to consumer reporting agencies 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 FURNISHERS OF INFORMATION:
OBLIGATIONS OF FURNISHERS UNDER THE FCRA

The federal Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681-1681y, imposes responsibilities on all persons who furnish information to consumer reporting agencies (CRAs). These responsibilities are found in Section 623 of the FCRA, 15 U.S.C. § 1681s-2. State law may impose additional requirements on furnishers. All furnishers of information to CRAs should become familiar with the applicable laws and may want to consult with their counsel to ensure that they are in compliance. The text of the FCRA is available at the website of the Consumer Financial Protection Bureau (CFPB): www.consumerfinance.gov/learnmore. A list of the sections of the FCRA cross-referenced to the U.S. Code is at the end of this document. Section 623 imposes the following duties upon furnishers:

Accuracy Guidelines
The FCRA requires furnishers to comply with federal guidelines and regulations dealing with the accuracy of information provided to CRAs by furnishers. Federal regulations and guidelines are available at www.consumerfinance.gov/learnmore. Section 623(e).

General Prohibition on Reporting Inaccurate Information
The FCRA prohibits information furnishers from providing information to a CRA that they know or have reasonable cause to believe is inaccurate. However, the furnisher is not subject to this general prohibition if it clearly and conspicuously specifies an address to which consumers may write to notify the furnisher that certain information is inaccurate. Sections 623(a) (1) (A) and (a) (1) (C).

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

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

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

Furnishers must comply with federal regulations that identify when an information furnisher must investigate a dispute made directly to the furnisher by a consumer. Under these regulations, furnishers must complete an investigation within 30 days (or 45 days, if the consumer later provides relevant additional information) unless the dispute is frivolous or irrelevant or comes from a "credit repair organization." Section 623(a) (8). Federal regulations are available at www.consumerfinance.gov/learnmore. Section 623(a) (8).

Duties After Notice of Dispute from Consumer Reporting Agency
If a CRA notifies a furnisher that a consumer disputes the completeness or accuracy of information provided by the furnisher, the furnisher has a duty to follow certain procedures. The furnisher must:

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

Duty to Report Voluntary Closing of Credit Accounts

Initial

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

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

Any person, such as a debt collector, that has acquired or is responsible for collecting delinquent accounts and that reports information to CRAs may comply with the requirements of Section 623(a)(5) (until there is a consumer dispute) by reporting the same delinquency date previously reported by the creditor. If the creditor did not report this date, they may comply with the FCRA by establishing reasonable procedures to obtain and report delinquency dates, or, if a delinquency date cannot be reasonably obtained, by following reasonable procedures to ensure that the date reported precedes the date when the account was placed for collection, charged to profit or loss, or subjected to any similar action. Section 623(a) (5).

Duties of Financial Institutions When Reporting Negative Information
Financial institutions that furnish information to "nationwide" consumer reporting agencies, as defined in Section 603(p), must notify consumers in writing if they may furnish or have furnished negative information to a CRA. Section 623(a) (7). The CFPB has prescribed model disclosures, 12 CFR Part 1022, App. B.

Duties When Furnishing Medical Information
A furnisher whose primary business is providing medical services, products, or devices (and such furnisher's agents or assignees) is a medical information furnisher for the purposes of the FCRA and must notify all CRAs to which it reports of this fact. Section 623(a) (9). This notice will enable CRAs to comply with their duties under Section 604(g) when reporting medical information.

Duties when ID Theft Occurs
All furnishers must have in place reasonable procedures to respond to notifications from CRAs that information furnished is the result of identity theft, and to prevent refurnishing the information in the future. A furnisher may not furnish information that a consumer has identified as resulting from identity theft unless the furnisher subsequently knows or is informed by the consumer that the information is correct. Section 623(a) (6). If a furnisher learns that it has furnished inaccurate information due to identity theft, it must notify each CRA of the correct information and must thereafter report only complete and accurate information. Section 623(a) (2). When any furnisher of information is notified pursuant to the procedures set forth in Section 605B that a debt has resulted from identity theft, the furnisher may not sell, transfer, or place for collection the debt except in certain limited circumstances. Section 615(f).

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

Exhibit "E"
Access Security Requirements

The following information security controls are required to reduce unauthorized access to consumer information. It is your company's responsibility to implement these controls. ONLINE 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 ONLINE's Services, Subscriber agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store ONLINE data.

1. Implement Strong Access Control Measures

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

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

1.3 If the third party or third party software or proprietary system or software, used to access ONLINE 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 ONLINE's infrastructure. Each user of the system access software must also have a unique logon password.

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

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

1.7 Develop strong passwords that are:
- Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
- Contain a minimum of eight (8) alphabetic and numeric characters for standard user accounts
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

1.8 Passwords (e.g. subscriber code passwords, user password) must be changed immediately when:
- Any system access software is replaced by another system access software or is no longer used
- The hardware on which the software resides is upgraded, changed or disposed
- Any suspicion of password being 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 Subscriber must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store ONLINE data.

1.14 Ensure that Subscriber 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 ONLINE 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 Subscriber'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. <u>Protect Data</u>

3.1 Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.).

3.2 ONLINE 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 ONLINE 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 ONLINE 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 ONLINE data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access ONLINE 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 ONLINE 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 ONLINE 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. <u>Maintain an Information Security Policy</u>

4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB 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 ONLINE data may have been compromised, immediately notify ONLINE within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Subscriber 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 ONLINE data, ensure that service provider is compliant with Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Subscriber responsibility to ensure the service provider is engaged with ONLINE and exception is granted in writing. *Approved certifications in lieu of E/3PA 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 ONLINE 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 ONLINE 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 ONLINE 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 ONLINE 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 ONLINE data on mobile devices is prohibited. Any exceptions must be obtained from ONLINE 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 ONLINE 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 ONLINE 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 ONLINE 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 ONLINE:
  ISO 27001, PCIDSS, EI3PA, SSAE 16- SOC 2, or SOC3, FISMA, CAI / CCM assessment

8. General

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

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

8.3 Subscriber shall be responsible for and ensure that third party software, which accesses ONLINE 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 Subscriber shall conduct software development (for software which accesses ONLINE information systems; this applies to both in-house and 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 ONLINE systems shall be made available to ONLINE upon request, for example during breach investigation or while performing audits

8.6 Data requests from Subscriber to ONLINE 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 Subscriber shall report actual security violations or incidents that impact ONLINE to ONLINE within twenty-four (24) hours or per agreed contractual notification timeline. Subscriber agrees to provide notice to ONLINE 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 800-234-7683, Email notification will be sent to tech@ONLINEis.com.

8.8 Subscriber acknowledges and agrees that the Subscriber (a) has received a copy of these requirements, (b) has read and understands Subscriber'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 ONLINE Services, systems or data, and (d) will abide by the provisions of these requirements when accessing ONLINE data.

8.9 Subscriber understands that its use of ONLINE networking and computing resources may be monitored and audited by ONLINE, without further notice.

8.10 Subscriber acknowledges and agrees that it is responsible for all activities of its employees/Authorized users, and for assuring that mechanisms to access ONLINE 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 ONLINE data, additional documentation may be required by ONLINE.

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, ONLINE requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 60 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, ONLINE 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 Subscriber and their employees or an authorized agent/s acting on behalf of the Subscriber are provided access to ONLINE provided Services via Internet ("Internet Access").

General requirements:

1. The Subscriber shall designate in writing, an employee to be its Head Security Designate, to act as the primary interface with ONLINE on systems access related matters. The Subscriber's Head Security Designate will be responsible for establishing, administering and monitoring all Subscriber employees' access to ONLINE provided Services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.

2. The Subscriber'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 ONLINE product based upon the legitimate business needs of each employee. ONLINE 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 Subscriber shall request employee's (Internet) user access via the Head Security Designate/Security Designate in writing, in the format approved by ONLINE. 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). ONLINE's approval of requests for (Internet) access may be granted or withheld in its sole discretion. ONLINE 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 Subscriber), 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 Subscriber agrees to notify ONLINE 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. Subscriber agrees to identify an employee it has designated to act on its behalf as a primary interface with ONLINE 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 Subscriber and shall be available to interact with ONLINE on information and product access, in accordance with these ONLINE Access Security Requirements. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Subscriber. Subscriber's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Subscriber'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 ONLINE's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to ONLINE immediately.
2. As a Client to ONLINE's products and Services via the Internet, the Head Security Designate is acting as the duly authorized representative of Subscriber.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Subscriber authorizes to act on behalf of the business in regards to ONLINE product access control (e.g. request to add/change/remove access). The Subscriber can opt to appoint more than one Security Designate (e.g. for backup purposes). The Subscriber understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with ONLINE's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding ONLINE 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 Subscriber, identified as an approval point for Subscriber's Authorized Users.
2. Is responsible for the initial and on-going authentication and validation of Subscriber'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 Subscriber's Authorized Users are authorized to access ONLINE products and Services.
5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Subscriber.
6. Must immediately report any suspicious or questionable activity to ONLINE regarding access to ONLINE's products and Services.
7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to ONLINE.
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 ONLINE 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.
IPAddress	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices- including routers, computers, time-servers, printers, Internet fax machines, and some telephones- must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Subscriber Code	Your seven digit ONLINE account number.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PAsr.' requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PAsr.' also establishes quarterly scans of networks for vulnerabilities.
ISO 27001/27002	IS 27001is 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.
PCIDSS	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 theElectronic 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.

Exhibit "F"
Death Master File Access Requirements

Subscriber agrees that based on its use of the Services that it may receive information for the Social Security Administrations Death Master File (DMF). Subscriber hereby warrants and agrees to the following requirements as users of the DMF.

a. Subscriber agrees to restrict Subscriber's use of deceased flags or other indicia within ONLINE's Services to legitimate fraud prevention or business purposes in compliance with applicable laws, rules and regulations and consistent with Subscriber's 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.

b. Subscriber certifies it will not take any adverse action against any consumer without further investigation to verify the information from the deceased flags or other indicia within ONLINE's Services.

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

d. Subscriber acknowledges that failure to comply with the provisions above may subject Subscriber 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. Subscriber shall indemnify and hold harmless the 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. Neither the Data Providers 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.

g. 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:

    a. 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,

Find that SSA already has the correct information on the main NUMIDENT file 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.

Initial

UTILITY EXCHANGE

Subscriber Service Application

Company Name: City of North Little Rock

Office Address: 120 Main Street

North Little Rock, Arkansas 72114

County: Pulaski County

Main Phone Number: 901-575-8888

Office Hours: 8:00AM-4:30PM Days of the week: Monday-Friday

Mailing Address: P.O. Box 936

North Little Rock, Arkansas 72114

Company Website: http://www.nlr.ar.gov

BANK REFERENCE

Bank Name: _____

Address: _____

City: _____

State: _____ Zip: _____

Bank Contact: _____ Phone: ( )

Account Number(s): _____

2 BUSINESS REFERENCES

(1)Business Name: _____

Address: _____

City: _____

State: _____ Zip: _____

Contact Person: _____ Phone: ( )

(2)Business Name: _____

Address: _____

City: _____

State: _____ Zip: _____

Contact Person: _____ Phone: ( )

PLEASE ANSWER THE FOLLOWING QUESTIONS

Industry:_____

Nature of Company's Business: _____

How long has company been in existence: _____years _____months

Will you be printing and storing reports? (Please check one) _____ Yes _____No
(If you will be printing and storing the ONLINE Utility Exchange Reports you are required to have them stored in a locking file cabinet)

Is your computer server in a locked room? (Please check one) _____Yes _____No

Do you have permanent signage at your office location that matches the company name on the Subscriber Agreement? (Please check one) _____Yes _____No

Do you lease or own your office location? (Please check one) _____Own _____Lease
(If you lease your office location, please provide a copy of your signed lease.)

Is office location a Commercial Building or Residence?_____

Do you have investigation License? (Please check one) ___Yes ___No

Estimated # of Credit Reports you will access monthly: _____

How will you access the Credit Report? (Please check one) ___ Personal Computer ___ Other

Is the company Tax Exempt? _____Yes _____ No If Yes, please provide tax exemption form.

_____
Signature

_____
Print Name/Title

_____
Date

Thank you for completing the application.

New Customer Setup Form

If you have any questions regarding how to fill out this form please contact your ONLINE Account Executive at (866) 630-6400.

BILLING/MONTHLY PAYMENT METHOD

Credit Card: Y / N Bank Draft: Y / N

Web Access Start Date: _____

Exchange Data Upload: Y/N

CUSTOMER INFORMATION SOFTWARE (CIS):

Software Vendor:_____ Version:_____

Will you be using the interface? Y / N

If ONLINE does not have an interface with your CIS provider currently please contact your ONLINE Account Executive to inquire about having one developed.

ACCESS SECURITY REQUIREMENT

ONLINE requires clients to utilize ONLINE's IP Address Restriction security feature. This prevents someone from obtaining user credentials and accessing information from outside your company's physical location. If you do not have static IP Addresses ONLINE has an alternate solution. Please check option below.

IP Address: _____

IP Address Range: _____ - _____

I do not have static IP Addresses ___.

DEPOSIT DECISIONING

Please fill out what you want your Score break points to be for your different deposit decisions. ONLINE has developed a default range setup. The default range setup is typically a good place for a utility to start when they may not have been using credit scores previously. Overtime you can utilize ONLINE's Statistical Reports and Score Adjust features to make changes. Please Check the Option Below

ONLINE'S DEFAULT SCORING _____			**CUSTOMIZE AS FOLLOWS _____ (Message Examples: Maximum, 2x Avg. Mo. Usage, Etc.)**
Green:	0.0%- 10.0%	Waive Deposit	**Green:** ____% - ____% **Deposit Message:** _____
Yellow:	10.1% - 25.0%	1X Average Monthly Usage	**Yellow:** ____% - ____% **Deposit Message:** _____
Red:	25.1% - 100.0%	2X Average Monthly Usage	**Red:** ____% - ____% **Deposit Message:** _____

There will be cases when a credit file will be unscoreable. An example would be for an applicant who maybe really young and may not have established enough credit yet. ONLINE has developed additional options to handle these types of credit files. Please circle your choices below.

No Score is Forced Decision: Yes/No (If Yes is chosen, complete options below)

No Score No Credit History: Red / Yellow / Green

No Score All Previous Credit History is Equally Positive and Negative: Red / Yellow / Green

No Score All Previous Credit History is Positive: Red / Yellow / Green

No Score All Previous Credit History is Negative: Red / Yellow / Green

No Score Previous Credit History is more Positive than Negative: Red / Yellow / Green

No Score Previous Credit History is more Negative than Positive: Red / Yellow / Green

ONLINE has developed client options on what decisions are returned on credit files which contain bankruptcy information. If you choose any option other than Default below, when a Bankruptcy, meeting your criteria, is on a credit file it will override the credit score decision and return the light decision you choose below.

Bankruptcy 7 Active: Default / Red / Yellow / Green

Bankruptcy 7 Discharged/Dismissed: Default / Red / Yellow / Green

Max Years to Consider Chapter 7: _____ years

Bankruptcy 13 Active: Default / Red / Yellow / Green

Bankruptcy 13 Discharged/Dismissed: Default / Red / Yellow / Green

Max Years to Consider Chapter 13: _____ years

ONLINE has developed additional logic which looks for specific types of accounts by industry on the credit file that you may want to force to a Red Light decision regardless of the credit score. If you choose anything other than Default it will override the credit score decision.

Unpaid Utility Debts: Default / Red

Unpaid Telecomm Debts: Default / Red

WEBSITE USER SETUP FORM

Score Visible: Y/N

(Certain Interfaces require these to match your CIS Package logins)

User Full Name	User Email Address	User Name	Administrator Supervisor User
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U

(If you need additional users setup please copy this page and submit with your contract package)

INTERFACE USER SETUP FORM

Score Visible to Users: Y/N

****Please contact your software vendor to get cost if any for interface set up****

User Full Name	User Email Address	Interface Login	Administrator Supervisor User
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U
			A/S/U

(If you need additional users setup please copy this page and submit with your contract package)

Customer Contacts

Inspection Contact Person:
Name:_____
PH:_____
Email:_____

Alternate Inspection Contact:
Name:_____
PH:_____
Email:_____

Training Contact:
Name:_____
PH:_____
Email:_____

Administrative Contact:
Name:_____
Title:_____
PH:_____
Receive Billing Y/N
FX:_____
Receive Announcements Y/N
Email:_____

Alternate Administrative Contact:
Name:_____
Title:_____
PH:_____
Receive Billing: Y/N
FX:_____
Receive Announcements: Y/N
Email:_____

Accounts Payable Contact:
(Responsible for Accounts Payable)
Name:_____
Title:_____
PH:_____
Receive Billing: Y/N
FX:_____
Receive Announcements: Y/N
Email:_____

Technical Contact:
(Responsible for IT/Data)
Name:_____
Title:_____
PH:_____
Receive Billing: Y/N
FX:_____
Receive Announcements: Y/N
Email:_____

(At least one contact must be setup to receive the monthly emailed invoice)

ON LINE
INFORMATION SERVICES

Recurring Monthly Payment Authorization Form

Schedule your payments to be automatically deducted from your bank account, or charged to your Visa, MasterCard, American Express or Discover Card. Just complete and sign this form to get started!

Here's How Recurring Payments Work:
You authorize regularly scheduled charges to your checking/savings account or credit card. You will be charged each billing period for the total amount due for that period. A paid in full invoice will be emailed to you and the charge will appear on your bank or credit card statement. You agree that no prior-notification will be provided. If the payment date changes, you will receive notice from us at least 10 days prior to the payment being collected.

Please complete the information below:

I _____ authorize ONLINE Information Services, Inc. on behalf of _____ _____ (Company) to charge/debit our account indicated below on the 5th business day of each month for payment of our ONLINE Information Services invoices.

Billing Address _____ Phone# _____

City, State, Zip _____ Email _____

Checking/ Savings Account

☐ Checking ☐ Savings

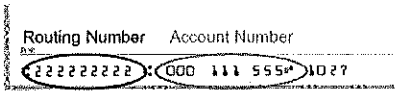
Name on Acct _____

Bank Name _____

Account Number _____

Bank Routing # _____

Bank City/State _____



Credit Card

☐ Visa ☐ MasterCard

☐ Amex ☐ Discover

Cardholder Name _____

Account Number _____

Exp. Date _____

CVV (3 digit number on back of card) _____

SIGNATURE _____ DATE _____

I understand that this authorization will remain in effect until I cancel it in writing, and I agree to notify ONLINE in writing of any changes in my account information or termination of this authorization at least 15 days prior to the next billing date. If the above noted payment dates fall on a weekend or holiday, I understand that the payments may be executed on the next business day. For ACH debits to my checking/savings account, I understand that because these are electronic transactions, these funds may be withdrawn from my account as soon as the above noted periodic transaction dates. In the case of an ACH Transaction being rejected for Non Sufficient Funds (NSF) I understand that ONLINE may at its discretion attempt to process the charge again within 30 days, and agree to an additional $25.00 charge for each attempt returned NSF which will be initiated as a separate transaction from the authorized recurring payment. I acknowledge that the origination of ACH transactions to my account must comply with the provisions of U.S. law. I certify that I am an authorized user of this credit card/bank account and will not dispute the scheduled transactions with my bank or credit card company; provided the transactions correspond to the terms indicated in this authorization form.

Initial