UNITED ONE FOR EVERY DECISION

Credit Services

Application and Exhibits A through I

In order to assure compliance with the Federal Fair Credit Reporting Act, Public Law 91-508 ("FCRA") and all other applicable laws, both state and federal, to cooperate with the other business and professional people in the confidential dissemination of credit information, and to assure the responsible use of credit information, the undersigned Applicant petitions United One Resources, Inc. d/b/a United One for the use of its service, and certifies to United One and agrees as follows:

Applicant Information:

Organization Name

Physical Address Suite/Floor

City State Zip Code

Contact Person First Name Last Name

☐ Same as Above

BILLING Address Suite/Floor

City State Zip Code

Phone Number Fax Number E-Mail

Web Address

Principals-List owner, Officer and/or Manager:

First Name Middle Name Last Name Title

Personal Address Apt/Floor

City State Zip Code SSN Year of Birth

First Name Middle Name Last Name Title

Personal Address Apt/Floor

City State Zip Code SSN Year of Birth

Organization Information:

Type of Business | Federal Id Number

Type of Ownership: ◯ Partnership ◯ Sole Owner ◯ Nonprofit ◯ Corporation ◯ LLC

Do you have any other company name(s) or DBA's? ◯ Yes ◯ No

If yes, please list:

Bank Reference

Account Numbers

Trade/Supplier Reference

In order to qualify for credit services, we understand that a current copy of our organizations business license will need to be submitted as part of the onboarding process.

☐ I agree that a copy of Business License will be submitted during the onboarding process.

Permissible Purpose /Appropriate Use, Must be Completed:

Application will not be processed unless this information is provided.

Each time a request for information or a credit report is made of United One, the Applicant's representative authorized to make such a request will use the information or report solely for a permissible purpose. Please describe the specific purpose for which Experian product information will be used. (What will you do with the information obtained?)

☐ Mortgage ☐ Home Equity ☐ Employment Screening ☐ Tenant Screening

Comments

Applicant will provide prompt, accurate and complete information at the time of transmission and will comply with §623 of the FCRA. Applicant may discuss information received from United One with the consumer in the event Applicant declines or takes adverse action regarding the consumer. In the event of disclosure to the consumer by Applicant, United One shall be held harmless by Applicant from any liability, damages, costs or expenses, including reasonable attorney's fees, resulting therefrom. United One shall not be liable in any manner whatsoever for any loss or injury to Applicant resulting from the obtaining or furnishing of such information and shall not be deemed to have guaranteed the accuracy of such information to be based, however, upon reports obtained from sources considered by United One to be reliable.

Exhibit A Subscriber Service Agreement

This agreement, dated below, is entered into by UNITED ONE RESOURCES, INC., a Pennsylvania Corporation, hereinafter known as "UNITED ONE" and

[ ] hereinafter referred to as "SUBSCRIBER", UNITED ONE and SUBSCRIBER agree as follows:

1. **SERVICES.** Provided SUBSCRIBER is not in default of any provision of this Agreement, UNITED ONE will furnish to SUBSCRIBER, on request, credit reports and other services, including but not limited to, court record services, flood zone determinations, appraisals, title insurance and settlement services, residential mortgage credit reports and prequalification reports. UNITED ONE will also (a) maintain files on individuals, firms or corporations, recording information furnished by it subscribers or obtained from other available sources; and (b) furnish all available pertinent information on individuals, firms or corporations, including but limited to, identifying information, credit history and employment and public record information in file --such information is being furnished at the special request of the SUBSCRIBER, as evidenced by the signature on this Agreement. UNITED ONE will not provide a record of inquiries in connection with credit or insurance transactions not initiated by the consumer.

2. **CHARGES AND INTEREST.** For each credit report or other service requested by SUBSCRIBER and provided by UNITED ONE, SUBSCRIBER agrees to pay UNITED ONE the applicable UNITED ONE charge then prevailing, in addition to any applicable service charges, dues or minimum billing rates. UNITED ONE will charge $40.00 for all returned checks. Such charges will be due thirty (30) days following the date of invoice. The balance of any invoice outstanding after such time shall be subject to a finance charge of 1.5% per month or the maximum finance charge permitted to be charged by applicable law, whichever is lower, and shall be immediately due and payable. SUBSCRIBER agrees that UNITED ONE's charges for credit reports and its other services are subject to change at any time without prior notice.

3. **UNITED ONE PERFORMANCE.** UNITED ONE will exercise all reasonable efforts to provide credit reports and any of its other services requested by SUBSCRIBER in an expeditious and efficient manner, but it shall have no liability to SUBSCRIBER for any delay or failure to do so.

4. **AUTHORIZATION, TRAINING AND COMPLIANCE WITH LAWS.** SUBSCRIBER shall maintain reasonable and appropriate procedures for authorizing any employee to request credit information and for the training of any employee involved in the use or reporting of credit information. SUBSCRIBER will ensure that all information will not be shared or forwarded with any third party. SUBSCRIBER will also maintain such procedures for compliance with all laws relating to the procurement or use of, or the furnishing of information for, credit reports, including, but not limited to, the Fair Credit Reporting Act, Public Law 91-508. SUBSCRIBER acknowledges that it is aware 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 that two (2) years, or both.

5. **TERM.** This Agreement shall continue in force without any fixed date of termination, but either UNITED ONE or SUBSCRIBER may terminate the Agreement upon giving ten (10) days prior written notice to the other. It is further agreed, however, that if the SUBSCRIBER is delinquent in the payment of any charge for credit reports or other services rendered by UNITED ONE for (60) days, or has breached any of the terms of this Agreement, UNITED ONE may, in its sole discretion, discontinue its services to SUBSCRIBER hereunder and cancel this Agreement immediately.

6. **FAIR CREDIT REPORTING ACT CERTIFICATION**. Subscriber certifies that it will order Equifax, Experian, and/or TranUnion Information Services that are consumer reports, as defined by the federal Fair Credit Reporting Act, 15 U.S.C. 1681 et soq. ("FCRA"), only when Subscriber intends to use that consumer report information: (a) in accordance with the FCRA and all state law counterparts: and (b) for the following permissible purposes: (i) in connection with a credit transaction involving the consumer on whom the consumer report is to be furnished and involving the extension of credit to. Subscriber will use each consumer report ordered under this Agreement for the foregoing purpose and for no other purpose.

7. **INDEMNIFICATION AND ATTORNEY'S FEES.** SUBSCRIBER shall indemnify, defend and hold UNITED ONE, all credit bureaus, Equifax, Experian, TransUnion and all their agents harmless from and against any and all claims, debts, demands damages, costs, expenses, fees, including attorney's fees, and any other liabilities which may be incurred by UNITED ONE based on any violation by the SUBSCRIBER of the Fair Credit Reporting Act or any other federal or state law or regulation pertaining to the procurement or use of a credit report or credit information (or the furnishing of information to a credit reporting agency) or pertaining to any of the other services provided by UNITED ONE to SUBSCRIBER under this Agreement. SUBSCRIBER shall also be liable for all of UNITED ONE'S attorney's fees and court costs incurred and other disbursements made in connection with the preparation, filing and prosecution of any lawsuit against SUBSCRIBER as a result of SUBSCRIBER's default of any provision of this Agreement.

8. **SUBSCRIBER ADDITIONS AND CHANGES.** This Agreement provides for services to any additional branches or departments within SUBSCRIBER's organization. SUBSCRIBER shall notify UNITED ONE of any address or telephone number changes, management changes, or any change in SUBSCRIBER's company name or ownership with thirty (30) days prior notice, and if requested by UNITED ONE will provide UNITED ONE with a revised SUBSCRIBER SERVICE AGREEMENT.

9. **SECTION HEADINGS.** The section headings in this Agreement are for convenience of reference only and are not a part of this Agreement, nor shall they be used to limit, expand or otherwise modify any term or condition of this Agreement.

10. **APPLICABLE LAW.** This Agreement shall be governed by and interpreted in accordance with the laws of the Commonwealth of Pennsylvania.

11. **JURISDICTION OVER DISPUTES.** SUBSCRIBER agrees that any dispute, controversy or claim arising under or in connection with this Agreement may be instituted by UNITED ONE in any court in which UNITED ONE has a place of business. For such purpose, SUBSCRIBER hereby submits to the personal jurisdiction of all such courts and further hereby waives any objection to such JURISDICTION and agrees that it shall be barred from asserting any such objection. SUBSCRIBER further hereby waives any right to assert or move for transfer of venue from any such court in which such action is instituted based on the doctrine of forum non conveniens or otherwise.

12. **ENTIRE AGREEMENT; INCORPORATION BY REFERENCE.** This Agreement sets forth the entire understanding and agreement between UNITED ONE and SUBSCRIBER and supersedes any prior oral or written agreements of the parties. This Agreement may be amended, supplemented or modified only by a written document executed by UNITED ONE and SUBSCRIBER. SUBSCRIBER hereby acknowledges that UNITED ONE has provided SUBSCRIBER with a copy of the Notice to Furnishers of Information: Obligations of Furnishers Under the FCRA and the Notice to Users of Consumer Reports: Obligations of Users under the FCRA, each in form as prescribed by the Federal Trade Commission. SUBSCRIBER also hereby acknowledges having executed UNITED ONE's Subscriber Compliance Certification form and Application for Service form, each of which are incorporated into this Agreement by reference and made a part hereof as if fully set forth at length herein.

13. **CALIFORNIA LAW CERTIFICATION.** Subscriber will refer to Exhibit F in making the following certification, and Subscriber agrees to comply with all applicable provisions of the California Credit Reporting Agencies Act.

(PLEASE SELECT THE APPROPRIATE LINE BELOW)

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

14. **VERMONT CERTIFICATION.** Subscriber certifies that it will comply with applicable provisions under Vermont law. In particular, Subscriber certifies that it will order information services relating to Vermont residents that are credit reports as defined by the Vermont Fair Credit Reporting Act ("VFCRA"), only after Subscriber has received prior consumer consent in accordance with VFCRA Section 2480e and applicable Vermont Rules. Subscriber further certifies that the attached copy of Section 2480e (Exhibit E) of the Vermont Fair Credit Reporting Statute was received from Equifax, Experian, and/or TranUnion.

Subscriber will comply with the applicable provisions of the FCRA, Federal Equal Credit Opportunity Act, Gramm-Leach-Bliley Act, and any amendments to them, all state law counterparts of them, and all applicable regulations promulgated under any of them including, without limitation, any provision requiring adverse action notification to the consumer.

15. **NO RESALE OF CREDIT REPORT.** Subscriber agrees that it will not resell any credit report.

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

Notice: The paragraph following this paragraph sets forth a warrant of authority for an attorney to confession against the SUBSCRIBER. In granting this warrant of authority to confess judgment against the SUBSCRIBER, the SUBSCRIBER hereby knowingly, intelligently, voluntarily, and, on advice of the separate legal counsel of the SUBSCRIBER, unconditionally waives any and all rights the undersigned has or may hereafter have to prior notice and an opportunity for a hearing under the respective constitutions and laws of the United States of America and of the Commonwealth of Pennsylvania.

SUBSCRIBER, to the fullest extent permitted by law, hereby irrevocably authorizes the Prothonotary, Clerk of Courts or any attorney of any court of record in the Commonwealth of Pennsylvania, or in any other state, to appear for SUBSCRIBER and confess judgment against SUBSCRIBER and in favor of UNITED ONE for the unpaid balance of any invoice described in Section 2 hereof and all accrued interest and other charges, costs and fees agreed to be paid by SUBSCRIBER hereunder with costs of suit and an attorney's commission of ten (10%) percent of all such sums (but in any event not less than $1,000), and with such expenses assessed from time to time as have been or are thereafter incurred by UNITED ONE for collection; and in so doing, this Agreement or a copy hereof verified by affidavit shall be sufficient warrant. The authority to confess judgment against SUBSCRIBER shall not be exhausted by one exercise thereof, but may be exercised from time to time and as often as UNITED ONE deems necessary or desirable until receiving full payment of all such invoice balances, accrued interest and other charges, costs and fees due and owing hereunder.

Guaranty: The obligation set forth in this Agreement is personally guaranteed by _____ (Guarantor), and guarantor hereby unconditionally guarantees the obligation set forth in this Agreement, and guarantees that the aforesaid obligations, conditions and covenants will be performed strictly in accordance with the terms of the contract, regardless of any law or regulation now or hereinafter in effect in any jurisdiction affecting the rights of United One Resources, Inc. with respect thereto, to the same effect as if the Guarantor had been the original signatory. The liability of Guarantor hereunder shall be absolute and unconditional irrespective of any circumstance which might otherwise constitute a defense or in discharge of Applicant/Subscriber or Guarantor. This guaranty is continuing and shall remain in full force and effect until fulfillment of all Applicant's /Subscriber's obligations, conditions and covenants under this contract, and is binding upon Guarantor's heirs, successors and/or assigns and shall remain in full force and effect until fulfillment of all conditions, obligations and covenants under said contract and shall inure for the benefit of United One Resources, Inc., its successors and/or assigns. No promises are made by United One Resources, Inc. to Guarantor to induce execution of this Guaranty.

WHEREFORE, UNITED ONE and SUBSCRIBER have caused this Agreement to be executed by their duly authorized representatives as of the date first written above.

IN WITNESS WHEREOF, End User and Provider have signed and delivered this Agreement.

Signature _____ Date _____

This application can not be processed without approval of Exhibits B and C.

Exhibit B Credit Scoring Service Agreement

This Credit Scoring Services Agreement, "Agreement", between _____ "End User" and United One Resources, Inc. d/b/a United One "Provider" agree as follows:

WHEREAS, Provider is an authorized reseller of Experian Information Solutions, Inc. (“Experian”); and

WHEREAS, Experian and Fair, Isaac Corporation (“Fair, Isaac”) offer the “Experian/Fair, Isaac Model”, consisting of the application of a risk model developed by Experian and Fair, Isaac which employs a proprietary algorithm and which, when applied to credit information relating to individuals with whom the End User contemplates entering into a credit relationship will result in a numerical score (the “Score” and collectively, “Scores”); the purpose of the models being to rank said individuals in order of the risk of unsatisfactory payment.

NOW, THEREFORE, For good and valuable consideration and intending to be legally bound, End User and Provider hereby agree as follows:

1. General Provisions

A. Subject of Agreement. The subject of this Agreement is End User's purchase of Scores produced from the Experian/Fair, Isaac Model from Provider.

B. Application. This Agreement applies to all uses of the Experian/Fair, Isaac Model by End User during the term of this agreement.

2. Experian/Fair, Isaac Scores

A. Generally. Upon request by End User during the Term, Provider will provide End User with the Scores.

B. Warranty. Provider warrants that the Scores are empirically derived and statistically sound predictors of consumer credit risk on the data from which they were developed when applied to the population for which they were developed. Provider further warrants that so long as it provides the Scores, the Scores will not contain or use any prohibited basis as defined by the Federal Equal Credit Opportunity Act, 15 USC Section 1691 et seq. or Regulation B promulgated thereunder. THE FOREGOING WARRANTIES ARE THE ONLY WARRANTIES PROVIDER HAS GIVEN END USER WITH RESPECT TO THE SCORES, AND SUCH WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, PROVIDER MIGHT HAVE GIVEN END USER WITH RESPECT THERETO, INCLUDING, FOR EXAMPLE, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. End User's rights under the foregoing warranties are expressly conditioned upon End User's periodic revalidation of the Experian/Fair, Isaac Model in compliance with the requirements of Regulation B as it may be amended from time to time (12 CFR Section 202 et seq.).

3. Release. End User hereby releases and holds harmless Provider, Fair Isaac and/or Experian and their respective officers, directors, employees, agents, sister or affiliated companies, and any third-party contractors or suppliers of Provider, Fair, Isaac or Experian from liability for any damages, losses, costs or expenses, whether direct or indirect, suffered or incurred by End User resulting from any failure of the Scores to accurately predict that a United States consumer will repay their existing or future credit obligations satisfactorily.

4.Intellectual Property

A. No License. Nothing contained in this Agreement shall be deemed to grant End User any license, sublicense, copyright interest, proprietary rights, or other claim against or interest in any computer programs utilized by Provider, Experian and/or Fair, Isaac or any third party involved in the delivery of the scoring services hereunder. End User acknowledges that the Experian/Fair, Isaac Model and its associated intellectual property rights in its output are the property of Fair, Isaac.

B. End User Use Limitations. By providing the Scores to End User pursuant to this Agreement, Provider grants to End User a limited license to use information contained in reports generated by the Experian/Fair, Isaac Model solely in its own business with no right to sublicense or otherwise sell or distribute said information to third parties. Before directing Provider to deliver Scores to any third party (as may be permitted by this Agreement), End User agrees to enter into a contract with such third party that (1) limits use of the Scores by the third party only to the use permitted to the End User, and (2) identifies Experian and Fair, Isaac as express third party beneficiaries of such contract.

C. Proprietary Designations. End User shall not use, or permit its employees, agents and subcontractors to use, the trademarks, service marks, logos, names, or any other proprietary designations of Provider, Experian or Fair, Isaac or their respective affiliates, whether registered or unregistered, without such party's prior written consent.

5. Compliance and Confidentiality

A. Compliance with Law. In performing this Agreement and in using information provided hereunder, End User will comply with all Federal, state, and local statutes, regulations, and rules applicable to consumer credit information and nondiscrimination in the extension of credit from time to time in effect during the Term of this contract. End User certifies that (1) it has a permissible purpose for obtaining the Scores in accordance with the Federal Fair Credit Reporting Act, and any similar applicable state statute, (2) any use of the Scores for purposes of evaluating the credit risk associated with applicants, prospects or existing customers will be in a manner consistent with the provisions described in the Equal Credit Opportunity Act ("ECOA"), Regulation B, and/or the Fair Credit Reporting Act, and (3) the Scores will not be used for Adverse Action as defined by the Equal Credit Opportunity Act ("ECOA") or Regulation B, unless adverse action reason codes have been delivered to the End User along with the Scores.

B. Confidentiality. End User will maintain internal procedures to minimize the risk of unauthorized disclosure of information delivered hereunder. End User will take reasonable precautions to assure that such information will be held in strict confidence and disclosed only to those of its employees whose duties reasonably relate to the legitimate business purposes for which the information is requested or used and to no other person. Without limiting the generality of the foregoing, End User will take suitable precautions to prevent loss, compromise, or misuse of any tapes or other media containing consumer credit information while in the possession of End User and while in transport between the parties. End User certifies that it will not publicly disseminate any results of the validations or other reports derived from the Scores without each of Experian's and Fair, Isaac's express written permission.

C. Proprietary Criteria. Under no circumstances will End User attempt in any manner, directly or indirectly, to discover or reverse engineer any confidential and proprietary criteria developed or used by Experian and/or Fair, Isaac in performing the scoring services hereunder.

D. Consumer Disclosure. Notwithstanding any contrary provision of this Agreement, End User may disclose the Scores provided to End User under this Agreement (1) to credit applicants, when accompanied by the corresponding reason codes, in the context of bona fide lending transactions and decisions only, and (2) as clearly required by law.

6. Indemnification and Limitations

A. Indemnification of Provider, Experian and Fair, Isaac. End User will indemnify, defend, and hold each of Provider, Experian and Fair, Isaac harmless from and against any and all liabilities, damages, losses, claims, costs, and expenses (including attorneys' fees) arising out of or resulting from any nonperformance by End User of any obligations to be performed by End User under this Agreement, provided that Experian/Fair, Isaac have given End User prompt notice of, and the opportunity and the authority (but not the duty) to defend or settle any such claim.

B. Limitation of Liability. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT, UNDER NO CIRCUMSTANCES WILL PROVIDER, EXPERIAN OR FAIR, ISAAC HAVE ANY OBLIGATION OR LIABILITY TO END USER FOR ANY INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES INCURRED BY END USER, REGARDLESS OF HOW SUCH DAMAGES ARISE AND OF WHETHER OR NOT END USER WAS ADVISED SUCH DAMAGES MIGHT ARISE. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF PROVIDER, EXPERIAN OR FAIR, ISAAC TO END USER EXCEED THE FEES PAID BY END USER PURSUANT TO THIS AGREEMENT DURING THE SIX MONTH PERIOD IMMEDIATELY PRECEDING THE DATE OF END USER'S CLAIM.

7. Miscellaneous

A. Third Parties. End User acknowledges that the Scores results from the joint efforts of Experian and Fair, Isaac. End User further acknowledges that each Experian and Fair, Isaac have a proprietary interest in said Scores and agrees that either Experian or the Fair, Isaac may enforce those rights as required.

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

Signature _____ Date _____

Addendum To Credit Reporting Services Agreement for OFAC Name Matching Service

This Addendum to the Credit Reporting Services Agreement for OFAC Matching Service ("Addendum") is made and entered into, by and between "Customer" and United One Resources, Inc. d/b/a United One, an Experian affiliate, a Pennsylvania Corporation, and Experian Information Solutions, Inc., an Ohio corporation, acting through its Information Solutions Division hereinafter referred to as "Experian".

WHEREAS, Customer and Experian have entered into the Credit Reporting Services Agreement and

WHEREAS, Customer and Experian mutually desire to amend the Agreement as set forth herein;

NOW, THEREFORE, in consideration of the foregoing and subject to the terms and conditions set forth herein, the parties hereto mutually agree as follows:

1. General Provisions

A .Application. This addendum sets forth the conditions under which Experian will provide Customer with the OFAC Name Matching Service (described below). This Addendum shall apply to all OFAC Name Matching Services performed by Experian for Customer during this Addendum. Prior to Experian's provision of the OFAC Name Matching Service to Customer, Customer agrees to the necessary agreements that will identify the nature and scope of the services provided hereunder, including any limitations set forth herein.

B. Term of this Addendum. This Addendum shall terminate upon the earlier of (i) the termination of the Agreement; or (ii) as otherwise set forth in the Agreement.

2. Charges to Customer. United One shall invoice and Customer agrees to pay United One the applicable charges set forth in the pricing proposal for the OFAC Name Matching Services rendered to Customer for each such inquiry to Experian's consumer credit reporting database.

3. OFAC Name Matching Service. For purposes of this Addendum, the term "OFAC Name Matching Service" means the application of a name matching service performed by Experian wherein the consumer's name transmitted by Customer inquiry or tape is compared to an Experian file containing limited identifying information of consumers listed by the United States Treasury Department, Office of Foreign Asset Control ("OFAC") of Specially Designated Nationals whose property is blocked, to assist the public in complying with the various sanctions programs administered by OFAC. Based upon Customer's Subscriber's request for consumer credit information, Experian will perform a match of characters in the consumer's name, social security number and year of birth, when available, and only where a match occurs, will Experian transmit to Customer's Subscriber's a message indicating the "Spelling of name used to access report matches OFAC List" in the on-line environment, and will only return a list of those consumers where a match occurs in the batch environment ("OFAC Statement").

4. Disclaimer of Warranty. Experian updates its file periodically from OFAC and cannot and will not, for the fee charged for the OFAC Name Matching Service, be an insurer or guarantor of the accuracy or reliability of the OFAC Name Matching Service nor the data contained in its file. Customer acknowledges and Customer will ensure that it's Subscribers acknowledge that the existence of a match based on very limited identifying information provided by OFAC does not necessarily indicate that the consumer for whom the Customer's Subscriber inquired is the same consumer referenced by OFAC. The use of the OFAC Name Matching Service does not attempt to, nor does it, satisfy any of Subscriber's legal obligations which may be administered by OFAC or any other governmental agency. EXPERIAN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE OFAC NAME MATCHING SERVICE, INCLUDING, FOR EXAMPLE AND WITHOUT LIMITATION, WARRANTIES OF CURRENTNESS, COMPLETENESS, ACCURACY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

5. Indemnification. Customer shall indemnify, defend and hold Experian harmless from and against any and all claims, liabilities and expenses, including responsible attorney's fees, which may be asserted against or incurred by Experian, that arise out of or are related to the use by Customer of the OFAC Name Matching Service.

6. Effect of Agreement. All terms and conditions of the Agreement not specifically addressed in the Addendum shall remain unchanged and in full force and effect. The Terms of this Addendum shall prevail in the event of any inconsistency between this Addendum and the Agreement.

7. Entire Understanding. This Credit Scoring Services Agreement and Addendum, set forth the entire understanding of the parties with respect to the subject matter hereof and supersede to the extent indicated all prior agreements, letters, convenants, arrangements, communications, representations and warranties, whether oral or written, by any employee, officer or representative of their party.

IN WITNESS WHEREOF, End User and Provider have signed and delivered this Agreement.

Signature Date

This application can not be processed without approval of Exhibit C.

Exhibit C End-User Agreement for Fair Isaac

In order to receive the Fair Isaac ClassicSM Credit Risk Score in conjunction with credit information obtained from the credit database(s) of Trans Union LLC from United One Resources, Inc. d/b/a United One "Reseller" [ ] "Subscriber" hereby agrees to the following terms:

1. Based on an agreement with Trans Union LLC ("Trans Union") and Fair Isaac Corporation ("Fair Isaac") ("Reseller Agreement"), Reseller has access to a unique and proprietary statistical credit scoring service jointly offered by Trans Union and Fair Isaac which evaluates certain information in the credit reports of individual consumers from Trans Union's data base ("Classic") and provides a score which rank orders consumers with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring (the "Classic Score").

2. Subscriber, from time to time, may desire to obtain Classic Scores from Trans Union via an on-line mode in connection with consumer credit reports.

3.Subscriber has previously represented and now, again represents that it is a [ ] and has a permissible purpose for obtaining consumer reports, as defined by Section 604 of the Federal Fair Credit Reporting Act (15 USC 1681b) including, without limitation, all amendments thereto ("FCRA").

4. Subscriber certifies that it will request Classic Scores pursuant to procedures prescribed by Reseller from time to time only for the permissible purpose certified above, and will use the Classic Scores obtained for no other purpose.

5. Subscriber will maintain copies of all written authorizations for a minimum of five (5) years from the date of inquiry.

6. Subscriber agrees that it shall use each Classic Score only for a one-time use and only in accordance with its permissible purpose under the FCRA.

7. With just cause, such as delinquency or violation of the terms of this contract or a legal requirement, Reseller may, upon its election, discontinue serving the Subscriber and cancel this Agreement, in whole or in part (e.g., the services provided under this Addendum only) immediately.

8. Subscriber recognizes that factors other than the Classic Score may be considered in making a credit decision. Such other factors include, but are not limited to, the credit report, the individual account history, and economic factors.

9. Trans Union and Fair Isaac shall be deemed third party beneficiaries under this Addendum.

10. Up to five score reason codes, or if applicable, exclusion reasons, are provided to Subscriber with Classic Scores. These score reason codes are designed to indicate the reasons why the individual did not have a higher Classic Score, and may be disclosed to consumers as the reasons for taking adverse action, as required by the Equal Credit Opportunity Act ("ECOA") and its implementing Regulation ("Reg. B"). However, the Classic Score itself is proprietary to Fair Isaac, may not be used as the reason for adverse action under Reg. B and, accordingly, shall not be disclosed to credit applicants or any other third party, except: (1) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or (2) as clearly required by law. Subscriber will not publicly disseminate any results of the validations or other reports derived from the Classic Scores without Fair Isaac and Trans Union's prior written consent.

11. In the event Subscriber intends to provide Classic Scores to any agent, Subscriber may do so provided, however, that Subscriber first enters into a written agreement with such agent that is consistent with Subscriber's obligations under this Agreement. Moreover, such agreement between Subscriber and such agent shall contain the following obligations and acknowledgments of the agent: (1) Such agent shall utilize the Classic Scores for the sole benefit of Subscriber and shall not utilize the Classic Scores for any other purpose including for such agent's own purposes or benefit; (2) That the Classic Score is proprietary to Fair Isaac and, accordingly, shall not be disclosed to the credit applicant or any third party without Trans Union and Fair Isaac's prior written consent except (a) to credit applicants in connection with approval/disapproval decisions in the context of bona fide credit extension transactions when accompanied with its corresponding score reason codes; or (b) as clearly required by law; (3) Such Agent shall not use the Classic Scores for model development, model validation, model benchmarking, reverse engineering, or model calibration; (4) Such agent shall not resell the Classic Scores; and (5) Such agent shall not use the Classic Scores to create or maintain a database for itself or otherwise.

12. Subscriber acknowledges that the Classic Scores provided under this Agreement which utilize an individual's consumer credit information will result in an inquiry being added to the consumer's credit file.

13. Subscriber shall be responsible for compliance with all applicable federal or state legislation, regulations and judicial actions, as now or as may become effective including, but not limited to, the FCRA, the ECOA, and Reg. B, to which it is subject.

14. The information including, without limitation, the consumer credit data, used in providing Classic Scores under this Agreement were obtained from sources considered to be reliable. However, due to the possibilities of errors inherent in the procurement and compilation of data involving a large number of individuals, neither the accuracy nor completeness of such information is guaranteed. Moreover, in no event shall Trans Union, Fair Isaac, nor their officers, employees, affiliated companies or bureaus, independent contractors or agents be liable to Subscriber for any claim, injury or damage suffered directly or indirectly by Subscriber as a result of the inaccuracy or incompleteness of such information used in providing Classic Scores under this Agreement and/or as a result of Subscriber's use of Classic Scores and/or any other information or serviced provided under this Agreement.

15.1 Fair Isaac, the developer of Classic, warrants that the scoring algorithms as delivered to Trans Union and used in the computation of the Classic Score ("Models") are empirically derived from Trans Union's credit data and are a demonstrably and statistically sound method of rank-ordering candidate records with respect to the relative likelihood that United States consumers will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring when applied to the population for which they were developed, and that no scoring algorithm used by Classic uses a "prohibited basis" as that term is defined in the Equal Credit Opportunity Act (ECOA) and Regulation B promulgated thereunder. Classic provides a statistical evaluation of certain information in Trans Union's files on a particular individual, and the Classic Score indicates the relative likelihood that the consumer will repay their existing or future credit obligations satisfactorily over the twenty four (24) month period following scoring relative to other individuals in Trans Union's database. The score may appear on a credit report for convenience only, but is not a part of the credit report nor does it add to the information in the report on which it is based.

15.2 THE WARRANTIES SET FORTH IN SECTION 15.1 ARE THE SOLE WARRANTIES MADE UNDER THIS ADDENDUM CONCERNING THE CLASSIC SCORES AND ANY OTHER DOCUMENTATION OR OTHER DELIVERABLES AND SERVICES PROVIDED UNDER THIS AGREEMENT; AND NEITHER FAIR ISAAC NOR TRANS UNION MAKE ANY OTHER REPRESENTATIONS OR WARRANTIES CONCERNING THE PRODUCTS AND SERVICES TO BE PROVIDED UNDER THIS AGREEMENT OTHER THAN AS SET FORTH IN THIS ADDENDUM. THE WARRANTIES AND REMEDIES SET FORTH IN SECTION 15.1 ARE IN LIEU OF ALL OTHERS, WHETHER WRITTEN OR ORAL, EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT MIGHT BE IMPLIED FROM A COURSE OF PERFORMANCE OR DEALING OR TRADE USAGE). THERE ARE NO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

16. IN NO EVENT SHALL ANY PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES INCURRED BY THE OTHER PARTIES AND ARISING OUT OF THE PERFORMANCE OF THIS AGREEMENT, INCLUDING BUT NOT LIMITED TO LOSS OF GOOD WILL AND LOST PROFITS OR REVENUE, WHETHER OR NOT SUCH LOSS OR DAMAGE IS BASED IN CONTRACT, WARRANTY, TORT, NEGLIGENCE, STRICT LIABILITY, INDEMNITY, OR OTHERWISE, EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

17. THE FOREGOING NOTWITHSTANDING, WITH RESPECT TO SUBSCRIBER, IN NO EVENT SHALL THE AFORESTATED LIMITATIONS OF LIABILITY, SET FORTH ABOVE IN SECTION 16, APPLY TO DAMAGES INCURRED BY TRANS UNION AND/OR FAIR ISAAC AS A RESULT OF: (A) GOVERNMENTAL, REGULATORY OR JUDICIAL ACTION(S) PERTAINING TO VIOLATIONS OF THE FCRA AND/OR OTHER LAWS, REGULATIONS AND/OR JUDICIAL ACTIONS TO THE EXTENT SUCH DAMAGES RESULT FROM SUBSCRIBER'S BREACH, DIRECTLY OR THROUGH SUBSCRIBER'S AGENT(S), OF ITS OBLIGATIONS UNDER THIS AGREEMENT.

18. ADDITIONALLY, NEITHER TRANS UNION NOR FAIR ISAAC SHALL BE LIABLE FOR ANY AND ALL CLAIMS ARISING OUT OF OR IN CONNECTION WITH THIS ADDENDUM BROUGHT MORE THAN ONE (1) YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED. IN NO EVENT SHALL TRANS UNION'S AND FAIR ISAAC'S AGGREGATE TOTAL LIABILITY, IF ANY, UNDER THIS AGREEMENT, EXCEED THE AGGREGATE AMOUNT PAID, UNDER THIS ADDENDUM, BY SUBSCRIBER DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING ANY SUCH CLAIM, OR TEN THOUSAND DOLLARS ($10,000.00), WHICHEVER AMOUNT IS LESS.

19. This Addendum may be terminated automatically and without notice: (1) in the event of a breach of the provisions of this Addendum by Subscriber; (2) in the event the agreement(s) related to Classic between Trans Union, Fair Isaac and Reseller are terminated or expire; (3) in the event the requirements of any law, regulation or judicial action are not met, (4) as a result of changes in laws, regulations or regulatory or judicial action, that the requirements of any law, regulation or judicial action will not be met; and/or (5) the use of the Classic Service is the subject of litigation or threatened litigation by any governmental entity.

IN WITNESS WHEREOF, End User and Provider have signed and delivered this Agreement.

Signature

Date

Print For Records

Once completed please return this application and agreements to:
onboarding@unitedone.com

For office use only

Date

Signed By

Exhibit D - End User Agreement For Equifax
Qualified Subscriber Terms and Conditions

Equifax Information Services (as defined below) will be received by Qualified Subscriber through Consumer Reporting Agency (CRA) subject to the following condition (the "Terms and Condition"):

1. Any information services and data originated from Equifax (the "Equifax Information Services" or "Equifax Information") will be requested only for Subscriber's exclusive use and held in strict confidence except to the extent that disclosure to others is required or permitted under the last sentence of this paragraph. Only designated representatives of Qualified Subscriber will request Equifax Information Services on Qualified Subscriber's employees, and employees are forbidden to obtain consumer reports on themselves, associates or any other persons except in the exercise of their official duties. Qualified Subscriber will not disclose Equifax Information to the subject of the report except as permitted or required by law, but will refer the subject to Equifax.

2. Qualified Subscriber will hold United One and all its agents harmless on account of any expense or damage arising or resulting from the publishing or other disclosure of Equifax Information by Qualified Subscriber, its employees or agents contrary to the conditions of Paragraph 1 or applicable law.

3. Recognizing that information for the Equifax Information Services is secured by and through fallible human sources and that, for the fee charged, United One cannot be an insurer of the accuracy of the Equifax Information Services, Qualified Subscriber understands that the accuracy of any Equifax Information Service received by Qualified Subscriber is not guaranteed by United One, and Qualified Subscriber releases United One and its affiliate companies, affiliated credit bureaus, agents, employees, and independent contractors from liability, even if caused by negligence, in connection with the Equifax Information Services and from any loss or expense suffered by Qualified Subscriber resulting directly or indirectly from Equifax Information.

4. Qualified Subscriber will be charged for the Equifax Information Services by United One, which is responsible for paying Equifax for the Equifax Information Services.

5. Written notices by either party to the other will terminate these Terms and Conditions effective ten (10) days after the date of that notice, but the obligations and agreements set forth in Paragraphs 1, 2, 3, 6 and 7 herein will remain in force.

6. Qualified Subscriber certifies that it will order Equifax Information Services that are consumer reports, as defined by the Federal Fair Credit Reporting Act, 15 U.S.C. 1681 et seq. ("FCRA"), only when Qualified Subscriber intends to use that consumer report information: (a) in accordance with the FCRA and all state law counterparts; and (b) for one of the following permissible purposes; (i) in connection with a credit transaction involving the consumer on whom the consumer report is to be furnished and involving the extension of credit to, or review or collection of an account of, the consumer; (ii) in connection with the underwriting of insurance involving the consumer; (iii) as a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation; (iv) when Qualified Subscriber otherwise has a legitimate business need for the information either in connection with a business transaction that is initiated by the consumer; or to review an account to determine whether the consumer continues to meet the terms of the accounts; or (v) for employment purposes; provided, however, that QUALIFIED SUBSCRIBER IS NOT AUTHORIZED TO REQUEST OR RECEIVE CONSUMER REPORTS FOR EMPLOYMENT PURPOSES UNLESS QUALIFIED SUBSCRIBER HAS AGREED IN WRITING TO THE TERMS AND CONDITIONS OF THE EQUIFAX PERSONA SERVICE. Qualified Subscriber will comply with the applicable provisions of the FCRA, Federal Equal Credit Opportunity Act, Gramm-Leach-Bliley Act and any amendments to them, all state law counterparts of them, and all applicable regulations promulgated under any of them including, without limitation, any provisions requiring adverse action notification to the consumer. Qualified Subscriber will use each consumer report ordered under these Terms and Conditions for one of the foregoing purposes and for no other purpose.

7. It is recognized and understood that the FCRA provides that anyone "who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under Title 18, United States Code, imprisoned for not more than two (2) years, or both." Equifax may periodically conduct audits of Qualified Subscriber regarding its compliance with these Terms and Conditions, including without limitations, the FCRA, other certifications and security provisions in these Terms and Conditions. Audits will be conducted by mail whenever possible and will require Qualified Subscriber to provide documentation as to permissible use of particular consumer reports. Qualified Subscriber gives the consent to Equifax to conduct such audits and agrees that any failure to cooperate fully and promptly in the conduct of any audit, or Qualified Subscriber's material breach of these Terms and Conditions, constitute grounds for immediate suspension of service or termination of these Terms and Conditions, notwithstanding Paragraph 5 above. If Equifax terminates these Terms and Conditions due to the conditions in the preceding sentence, Qualified Subscriber (i) unconditionally releases and agrees to hold United One harmless and indemnify it from and against any and all liabilities of whatever kind or nature that may arise from or related to such termination, and (ii) covenants it will not assert any claim or cause of action of any kind or

8. Data Security

8.1 This Paragraph 8 applies to any means through which Qualified Subscriber orders or accesses the Equifax Information Services including, without limitation, system-to-system, personal computer or the Internet; provided, however, if Qualified Subscriber orders or accesses the Equifax Information Services via the Internet, Qualified Subscriber shall fully comply with Equifax's connectivity security requirements specified in Paragraph 8.3, below.

For the purposes of this Paragraph 8, the term “Authorized User” means a Qualified Subscriber employee that Qualified Subscriber has authorized to order or access the Equifax information Services and who is trained on Qualified Subscriber's obligation under these Terms and Conditions with respect to the ordering and used of the Equifax Information Services, and the information provided through same, including Qualified Subscriber's FCRA and other obligations with respect to the access and use of consumer reports.

8.2 Qualified Subscriber will, with respect to handling Equifax Information:

(a) Ensure that only Authorized Users can order or have access to the Equifax Information Services.

(b) Ensure that Authorized Users do not order credit reports for personal reasons or provide them to any third party except as permitted by these Terms and Conditions.

(c) Ensure that all devices used by Qualified Subscriber to order or access the Equifax Information Services are placed in a secure location and accessible only by Authorized Users, and that such devices are secured when not in use through such means as screen locks, shutting power controls off, or other commercially reasonable security procedure.

(d) Take all necessary measures to prevent unauthorized ordering of or access to the Equifax Information Services by any person other than an Authorized User for permissible purposes, including, without limitation, limiting the knowledge of the Qualified Subscriber security codes, member numbers, User IDs, and any passwords Qualified Subscriber may use, to those individuals with a need to know, changing Qualified Subscriber's user passwords at least every ninety (90) days, or sooner if an Authorized User is no longer responsible for accessing the Equifax Information Services, or if Qualified Subscriber suspects an unauthorized person has learned the password, and using all security features in the software and hardware Qualified Subscriber uses to order or access the Equifax Information Services.

(e) In no event access the Equifax Information Services via any wireless communication device, including but not limited to, web enabled cell phones, interactive wireless pagers, personal digital assistants (PDAs), mobile data terminals and portable data terminals.

(f) Not use personal computer hard drives or portable and/or removable data storage equipment or media (including but not limited to laptops, zip drives, tapes, disks, CDs, DVDs, software, and code) to store the Equifax Information Services. In addition, Equifax Information must be encrypted when not in use and all printed Equifax Information must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose.

(g) If Qualified Subscriber sends, transfers or ships any Equifax Information, encrypt the Equifax Information using the following minimum standards, which standards may be modified from time to time by Equifax; Advanced Encryption Standard (AES), minimum 128-bit key or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms.

(h) Monitor compliance with the obligations of this Paragraph 8, and immediately notify Equifax if Qualified Subscriber suspects or knows of any unauthorized access or attempt to access the Equifax Information Services. Such monitoring will include, without limitation, a review of each CRA invoice for the purpose of detecting any unauthorized activity.

(i) Not ship hardware or software between Qualified Subscriber's locations or to third parties without deleting all Equifax Qualified Subscriber number(s), security codes, User IDs, passwords, Qualified Subscriber user passwords, and any consumer information.

(j) Access, use and store the Information Services (for purposes of this Paragraph 8 “Information Services” shall include without limitation all information and data provided or obtained through use of the Information Services) only at or from locations within the territorial boundaries of the United States, United States territories and Canada (the “Permitted Territory”). Qualified Subscriber may not access, use or store the Information Services at or from, or send the Information Services to, any location outside of the Permitted Territory without first obtaining Equifax's written permission.

(k) Inform Authorized Users that unauthorized access to consumer reports may subject them to civil and criminal liability under the FCRA punishable by fines and imprisonment.

(l) Use commercially reasonable efforts to assure data security when disposing of any consumer report information or record obtained from Equifax. Such efforts must include the use of those procedures issued by the federal regulatory agency charged with oversight of Qualifies Subscriber's activities (e.g. the Federal Trade Commission, the applicable banking or credit union regulator) applicable to the disposal of consumer report information or records.

8.3 Qualified Subscriber will, with respect to Qualified Subscriber's network security:

(a) Use commercially reasonable efforts to protect Equifax Information when stored on servers, subject to the following requirements: (i) Equifax Information must be protected by multiple layers of network security, including but not limited to firewalls, routers, and intrusion detection devices; (ii) secure access (both physical and network) to systems storing Equifax Information, must include authentication and passwords that are changed at least every 90 days; and (iii) all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available.

(b) Use commercially reasonable efforts to protect Qualified Subscriber's connection with dedicated, industry-recognized firewalls that are configured and managed to adhere to industry accepted best practices.

(c) Only hold Equifax Information on an application server which can only be accessed by a presentation server, through one of the following: (i) Dual or multiple firewall method (preferred) - this method consists of a firewall between the internet and the presentation server(s) and another firewall between the presentation server(s) and the application server holding Equifax Information. The network firewall should ensure that only the presentation server(s) is/are allowed to access the application server holding Equifax information, (ii) Single firewall method (acceptable) - when a dual firewall method is not feasible, a single firewall will provide acceptable levels of protection. The firewall should be installed between the internet and the presentation server(s). Multiple interfaces to separate the presentation server(s) and the application server holding Equifax Information are required. The firewall should be configured to allow only the presentation server(s) access to the application server holding Equifax Information, or (iii) ensure that all administrative and network access to the firewalls and servers must be through an internal network or protected extranet using strong authentication encryption such as VPN and SSH.

(d) Use commercially reasonable efforts to route communications from Qualified Subscriber's internal services to external systems through firewalls configured for network address translation (NAT).

(e) Use commercially reasonable efforts to establish procedures and logging mechanism for systems and networks that will allow tracking and analysis in the event there is a compromise, and maintain an audit trail history for at least three (3) months for review by Equifax.

8.4 If Equifax reasonably believes that Qualified Subscriber has violated this Paragraph 8, Equifax may, in addition to any other remedy authorized by these Terms and Conditions, with reasonable advance written notice to Qualified Subscriber and at Equifax's sole expense, conduct, or have a third party conduct on its behalf, an audit of Qualified Subscriber's network security systems, facilities, practices and procedures to the extent Equifax reasonably deems necessary, including an on-site inspection, to evaluate Qualified Subscriber's compliance with the data security requirements of this Paragraph 8.

9. These Terms and Conditions will be governed by and construed in accordance with the laws of the State of Pennsylvania without giving effect to its conflicts of laws provisions. These Terms and Conditions constitute the entire agreement of the parties with respect to Qualified Subscriber receiving Equifax Information Services and no changes in these Terms and Conditions may be made except in writing by an officer of United One.

Signature

Date

Exhibit E
End User Certification of Compliance

Vermont Fair Credit Reporting Contract Certification

This is to remind you of Vermont's Fair Credit Reporting statute, 9 V.S.A sec 2480e, and FCR rule CF 112, and to request your written certification that you are in compliance with the applicable section of this law. Vermont's statutes and rules differ from the Federal Fair Credit Reporting Act, and require a credit report user to obtain the consumer's consent prior to accessing a credit report.

The undersigned, ("customer") acknowledges that it subscribes to receive various information services from S.I.R. in accordance with the Vermont Fair Credit reporting Statute , 9V.S.A. sec 2480e (1999), as amended (the "FCRA") and its other state law counterparts. In connection with Customer's continued use of S.I.R. services in relation to Vermont consumers, the Customer hereby certifies as follows.

Customer certifies that it will comply with applicable provisions under Vermont Law. In particular, Customer certifies that it will order information services relating to Vermont residents that are credit reports as defined by the VFCRA, only after customer has received prior consumer consent in accordance with VFCRA sec 2480e and applicable Vermont rules.

Signature

Date/Time Field

Exhibit F
End User Certification of Compliance

California Civil Code - Section 1785.14(a)

Section 1785.4(a), as amended, states that a consumer credit reporting agency does not have reasonable grounds for believing that a consumer credit report will only be used for a permissible purpose unless all of the following requirements are met:

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

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

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

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

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

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

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

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

Signature Date/Time Field

Exhibit G

Access Security Requirements for Reseller End-Users for FCRA and GLB 5A Data

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

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

1. Implement Strong Access Control Measures

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

1.2 If using third party or proprietary system to access United One'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 United One data/systems.

1.3 If the third party or third party software or proprietary system or software, used to access United One 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 United One'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, and
- For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended).

1.8 Passwords (e.g. user/account password) must be changed immediately when:

- Any system access software is replaced by another system access software or is no longer used,
- The hardware on which the software resides is upgraded, changed or disposed, and
- Any suspicion of password being disclosed to an unauthorized party (see section 4.3 for reporting requirements).

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

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

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

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

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

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

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

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

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

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

2. Maintain a Vulnerability Management Program

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

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

2.3 Implement and follow current best security practices for computer virus detection scanning services and procedures:

- Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.
- Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.
- If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

3. Protect Data

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

3.2 Experian data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.

3.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all Experian data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

3.5 Experian data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access Experian data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Experian data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing Experian data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing Experian data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

4. Maintain an Information Security Policy

4.1 Develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.

4.3 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators. *If you believe Experian data may have been compromised, immediately notify United One within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Company implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers) to access, transmit, store or process Experian data, ensure that service provider is compliant with the Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian's list of compliant service providers. If the service provider is in the process of becoming compliant, it is Company's responsibility to ensure the service provider is engaged with Experian and an exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*

5. Build and Maintain a Secure Network

5.1 Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.

5.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.

5.3 Administrative access to firewalls and servers must be performed through a secure internal wired connection only.

5.4 Any stand-alone computers that directly access the Internet must have a desktop firewall deployed that is installed and configured to block unnecessary/unused ports, services, and network traffic.

5.5 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of Experian data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers (e.g. software providers) to access United One systems, access to third party tools/ services must require multi-factor authentication.

6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)

6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Experian data; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.

6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access United One 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
- and protecting against intrusions of operating systems or software.

7.Mobile and Cloud Technology

7.1 Storing Experian data on mobile devices is prohibited. Any exceptions must be obtained from Experian in writing; additional security requirements will apply.

7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.

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

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

7.5 Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Experian data to be exchanged between secured and non-secured applications on the mobile device.

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

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

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

8. General

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

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

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

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

- **8.4.1** Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.
- **8.4.2** Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.
- **8.4.3** Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

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

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

8.7 Company shall report actual security violations or incidents that impact Experian to United One within twenty-four (24) hours or per agreed contractual notification timeline. Company agrees to provide notice to United One 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 570-706-2987, email notification will be sent to sbiagioli@unitedone.com.

8.8 Company acknowledges and agrees that the Company (a) has received a copy of these requirements, (b) has read and understands Company's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to United One services, systems or data, and (d) will abide by the provisions of these requirements when accessing Experian data.

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

8.10 Company acknowledges and agrees that it is responsible for all activities of its employees/authorized users, and for assuring that mechanisms to access United One services or data are secure and in compliance with its membership agreement.

8.11 When using third party service providers to access, transmit, or store Experian data, additional documentation may be required by United One.

Record Retention: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, Experian requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a consumer complaint that your company impermissibly accessed their credit report, Experian will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.

"Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than $3,500 per violation."

Internet Delivery Security Requirements

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

General requirements:

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

Roles and Responsibilities

1. Company agrees to identify an employee it has designated to act on its behalf as a primary interface with United One on systems access related matters. This individual shall be identified as the "Head Security Designate." The Head Security Designate can further identify a Security Designate(s) to provide the day to day administration of the Authorized Users. Security Designate(s) must be an employee and a duly appointed representative of the Company and shall be available to interact with United One on information and product access, in accordance with these Experian Access Security Requirements for Reseller End-Users. The Head Security Designate Authorization Form must be signed by a duly authorized representative of the Company. Company's duly authorized representative (e.g. contracting officer, security manager, etc.) must authorize changes to Company's Head Security Designate. The Head Security Designate will submit all requests to create, change or lock Security Designate and/or Authorized User access accounts and permissions to United One's systems and information (via the Internet). Changes in Head Security Designate status (e.g. transfer or termination) are to be reported to United One immediately.
2. As a Client to United One's products and services via the Internet, the Head Security Designate is acting as the duly authorized representative of Company.
3. The Security Designate may be appointed by the Head Security Designate as the individual that the Company authorizes to act on behalf of the business in regards to United One product access control (e.g. request to add/change/remove access). The Company can opt to appoint more than one Security Designate (e.g. for backup purposes). The Company understands that the Security Designate(s) it appoints shall be someone who will generally be available during normal business hours and can liaise with United One's Security Administration group on information and product access matters.
4. The Head Designate shall be responsible for notifying their corresponding United One representative in a timely fashion of any Authorized User accounts (with their corresponding privileges and access to application and data) that are required to be terminated due to suspicion (or actual) threat of system compromise, unauthorized access to data and/or applications, or account inactivity.

Designate

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

Signature

Date

Print Name/Title

Company Name

Glossary

Term	Definition
Computer Virus	A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying.
Confidential	Very sensitive information. Disclosure could adversely impact your company.
Encryption	Encryption is the process of obscuring information to make it unreadable without special knowledge.
Firewall	In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle.
Information Lifecycle	(Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained.
IP Address	A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices.
Peer-to-Peer	A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission.
Router	A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets.
Spyware	Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet.
Experian Independent Third Party Assessment Program	The Experian Independent 3rd Party Assessment is an annual assessment of an Experian Reseller's ability to protect the information they purchase from Experian. EI3PA requires an evaluation of a Reseller's information security by an independent assessor, based on requirements provided by Experian. EI3PA also establishes quarterly scans of networks for vulnerabilities.
ISO 27001 /27002	IS 27001 is the specification for an ISMS, an Information Security Management System (it replaced the old BS7799-2 standard) The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001.
PCI DSS	The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.
SSAE 16 SOC 2, SOC3	Statement on Standards for Attestation Engagements (SSAE) No. 1 SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy. The SOC 3 Report , just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material).
FISMA	The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002.
CAI / CCM	Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments. The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider.

Exhibit H

FCRA Requirements

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

Although the FCRA primarily regulates the operations of consumer credit reporting agencies, it also affects you as a user of information. We have included a copy of the FCRA with your membership kit. We suggest that you and your 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

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

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

We strongly endorse the letter and spirit of the Federal Fair Credit Reporting Act. We believe that this law and similar state laws recognize and preserve the delicate balance between the rights of the consumer and the legitimate needs of commerce.

In addition to the Federal Fair Credit Reporting Act, other federal and state laws addressing such topics as computer crime and unauthorized access to protected databases have also been enacted. As a prospective user of consumer reports, we expect that you and your staff will comply with all relevant federal statutes and the statutes and regulations of the states in which you operate. We support consumer reporting legislation that will assure fair and equitable treatment for all consumers and users of credit information.

I have read and understand the “Access Security Requirements” and “FCRA Requirements” notice and will take all reasonable measures to enforce them within my facility. I certify that I will use all product(s) information for no other purpose than what is stated in the Permissible Purpose/Appropriate Use section that has been approved and for my type of business. I will not resell or distribute the reports to any third party that is not fully vetted and contracted by my organization.

*Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses may be fined under Title 18, United States Code, imprisoned for not more than 2 years, or both. United One Resources' reserves the right to work directly with law enforcement to enforce this statute and other criminal statutes.

NOTE: Access to ANY consumer credit report is ONLY for the Permissible Purpose(s) on your Application for Service in the Permissible Purpose/ Appropriate Use Section. Consumer credit reports may NOT be accesses for personal information, curiosity, divorce or other reasons outside the Permissible Purposes recognized for your specific business use(s) outlined at the time of Onboarding.

Signature

Date

Exhibit I
IMPORTANT NOTICE

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

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

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

Signature

Date

Print Name

Company Name