Exhibit I: LexisNexis Risk Solutions | Contractor's Terms & Conditions

LexisNexis Master Terms and Conditions (form LNMTC) – Government (Document 1)

These LexisNexis Master Terms and Conditions (form LNMTC) (the "**Master Terms**") are entered into as of (the "**Effective Date**"), by and between **LexisNexis Risk Solutions Bureau LLC ("LNRSB") and LexisNexis Risk Solutions FL Inc.** ("**LNRSFL**"), with their principal place of business located at 1000 Alderman Drive, Alpharetta, Georgia 30005 and ("**Customer**"), with its principal place of business located at , each individually referred to as the "**Party**" and collectively as the "**Parties**." These Master Terms govern the provision of the LN Services (as defined below) by LNRSFL, LNRSB and each of their respective Affiliates who provide LN Services under these Master Terms (collectively referred to as "**LN**").

WHEREAS, LNRSB (as defined below) is a consumer reporting agency in the business of providing consumer reports (the "**FCRA LN Services**") which are governed by the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("**FCRA**"); and

WHEREAS, LNRSFL is the provider of certain data products, data applications and other related services not governed by the FCRA (the "**Non-FCRA LN Services**"); and

WHEREAS, Customer is a company requesting such data and data related services and is desirous of receiving LN's capabilities; and

WHEREAS, the Parties now intend for these Master Terms to be the master agreement governing the relationship between the Parties with respect to the FCRA LN Services and/or the Non-FCRA LN Services (individually and collectively, also referred to as the "**LN Services**") as of the Effective Date.

NOW, **THEREFORE**, LN and Customer agree to be mutually bound by the terms and conditions of these Master Terms, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, do hereby agree as follows:

1. SCOPE OF SERVICES/CUSTOMER CREDENTIALING. Subject to the terms of the Subscription Agreement, LN agrees to provide the LN Services described in such Subscription Agreement to Customer, subject to the terms and conditions herein. References to the LN Services shall also be deemed to include the data therein as well as any Software provided by LN. These Master Terms shall encompass any and all delivery methods provided to Customer for the LN Services, including, but not limited to, online, batch, XML, assisted searching, machine-to-machine searches, and any other means which may become available. Customer acknowledges and understands that LN will only allow Customer access to the LN Services if Customer's credentials can be verified in accordance with LN's internal credentialing procedures. The foregoing shall also apply to the addition of Customer's individual locations and/or accounts.

2. RESTRICTED LICENSE. LN hereby grants to Customer a restricted license to use the LN Services, subject to the restrictions and limitations set forth below:

(i) Generally. LN hereby grants to Customer a restricted license to use the LN Services solely for Customer's own internal business purposes. Customer represents and warrants that all of Customer's use of the LN Services shall be for only legitimate business purposes, including those specified by Customer in connection with a specific information request, relating to its business and as otherwise governed by the Master Terms. Customer shall not use the LN Services for marketing purposes or resell or broker the LN Services to any third party, and shall not use the LN Services for personal (non-business) purposes. Customer

shall not use the LN Services to provide data processing services to third parties or evaluate data for third parties or, without LN's consent, to compare the LN Services against a third party's data processing services. Customer agrees that, if LN determines or reasonably suspects that continued provision of LN Services to Customer entails a potential security risk, or that Customer is in violation of any provision of these Master Terms or law, LN may take immediate action, including, without limitation, terminating the delivery of, and the license to use, the LN Services. Customer shall not access the LN Services from Internet Protocol addresses located outside of the United States and its territories without LN's prior written approval. Customer may not use the LN Services to create a competing product. Customer shall comply with all laws, regulations and rules which govern the use of the LN Services and information provided therein. LN may at any time mask or cease to provide Customer access to any LN Services or portions thereof which LN may deem, in LN's sole discretion, to be sensitive or restricted information.

(ii) GLBA Data. Some of the information contained in the LN Services is "nonpublic personal information," as defined in the Gramm-Leach-Bliley Act, (15 U.S.C. § 6801, et seq.) and related state laws (collectively, the "**GLBA**"), and is regulated by the GLBA ("**GLBA Data**"). Customer shall not obtain and/or use GLBA Data through the LN Services in any manner that would violate the GLBA, or any similar state or local laws, regulations and rules. Customer acknowledges and agrees that it may be required to certify its permissible use of GLBA Data falling within an exception set forth in the GLBA at the time it requests information in connection with certain LN Services and will recertify upon request by LN. Customer certifies with respect to GLBA Data received through the LN Services that it complies with the Interagency Standards for Safeguarding Customer Information issued pursuant to the GLBA.

(iii) DPPA Data. Some of the information contained in the LN Services is "personal information," as defined in the Drivers Privacy Protection Act, (18 U.S.C. § 2721 et seq.) and related state laws (collectively, the "**DPPA**"), and is regulated by the DPPA ("**DPPA Data**"). Customer shall not obtain and/or use DPPA Data through the LN Services in any manner that would violate the DPPA. Customer acknowledges and agrees that it may be required to certify its permissible use of DPPA Data at the time it requests information in connection with certain LN Services and will recertify upon request by LN.

(iv) Social Security and Driver's License Numbers. LN may in its sole discretion permit Customer to access full social security numbers (nine (9) digits) and driver's license numbers (collectively, "**QA Data**"). If Customer is authorized by LN to receive QA Data, and Customer obtains QA Data through the LN Services, Customer certifies it will not use the QA Data for any purpose other than as expressly authorized by LN policies, the terms and conditions herein, and applicable laws and regulations. In addition to the restrictions on distribution otherwise set forth in Paragraph 3 below, Customer agrees that it will not permit QA Data obtained through the LN Services to be used by an employee or contractor that is not an Authorized User with an Authorized Use. Customer agrees it will certify, in writing, its uses for QA Data and recertify upon request by LN. Customer may not, to the extent permitted by the terms of these Master Terms, transfer QA Data via email or ftp without LN's prior written consent. However, Customer shall be permitted to transfer such information so long as: 1) a secured method (for example, sftp) is used, 2) transfer is not to any third party, and 3) such transfer is limited to such use as permitted under these Master Terms. LN may at any time and for any or no reason cease to provide or limit the provision of QA Data to Customer.

(v) Copyrighted and Trademarked Materials. Customer shall not remove or obscure any trademarks, copyright notices or other notices contained on materials accessed through the LN Services.

(vi) Additional Terms. To the extent that the LN Services accessed by Customer include information or data described in the Risk Supplemental Terms contained in Appendix I, attached hereto, Customer agrees to comply with the Risk Supplemental Terms set forth therein. Additionally, certain other information contained within the LN Services is subject to additional obligations and restrictions. These services include, without

limitation, news, business information, and federal legislative and regulatory materials. To the extent that Customer receives such news, business information, and federal legislative and regulatory materials through the LN Services, Customer agrees to comply with the Terms and Conditions contained in Appendix II, attached hereto (the "**L&P Terms**"). The Risk Supplemental Terms and the L&P Terms are hereby incorporated into these Master Terms by reference. In the event of a direct conflict between these Master Terms, the Risk Supplemental Terms, and the L&P Terms, the order of precedence shall be as follows: these Master Terms, the Risk Supplemental Terms and then the L&P Terms.

(vii) MVR Data. If Customer is permitted to access Motor Vehicle Records ("**MVR Data**") from LN, without in any way limiting Customer's obligations to comply with all state and federal laws governing use of MVR Data, the following specific restrictions apply and are subject to change:

(a) Customer shall not use any MVR Data provided by LN, or portions of information contained therein, to create or update a file that Customer uses to develop its own source of driving history information.
(b) As requested by LN, Customer shall complete any state forms that LN is legally or contractually bound to obtain from Customer before providing Customer with MVR Data.
(c) LN (and certain third-party vendors) may conduct reasonable and periodic audits of Customer's use of MVR Data. In response to any such audit, Customer must be able to substantiate the reason for each MVR Data order.

(viii) HIPAA. Customer represents and warrants that Customer will not provide LN with any Protected Health Information (as that term is defined in 45 C.F.R. Sec. 160.103) or with Electronic Health Records or Patient Health Records (as those terms are defined in 42 U.S.C. Sec. 17921(5), and 42 U.S.C. Sec. 17921(11), respectively) or with information from such records without the execution of a separate agreement between the parties.

(ix) Economic Sanctions Laws. Customer acknowledges that LN is subject to economic sanctions laws, including but not limited to those enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control ("**OFAC**"), the European Union, and the United Kingdom. Accordingly, Customer shall comply with all economic sanctions laws of the United States, the European Union, and the United Kingdom. Customer shall not provide access to LN Services to any individuals identified on OFAC's list of Specially Designated Nationals ("**SDN List**"), the UK's HM Treasury's Consolidated List of Sanctions Targets, or the EU's Consolidated List of Persons, Groups, and Entities Subject to EU Financial Sanctions. Customer shall not take any action which would place LN in a position of non-compliance with any such economic sanctions laws.

(x) Retention of Records. For uses of GLB Data, DPPA Data and MVR Data, as described in Sections 2(ii), 2(iii) and 2(vii), Customer shall maintain for a period of five (5) years a complete and accurate record (including consumer identity, purpose and, if applicable, consumer authorization) pertaining to every access to such data.

(xi) Software. To the extent that Customer is using software provided by LN ("**Software**"), whether hosted by LN or installed on Customer's equipment, such Software shall be deemed provided under a limited, revocable license, for the sole purpose of using the LN Services. In addition, the following terms apply: Customer shall not (a) use the Software to store or transmit infringing, libelous, or otherwise unlawful or tortuous material, or to store or transmit material in violation of third-party privacy rights, (b) use the Software to store or transmit spyware, adware, other malicious programs or code, programs that infringe the rights of others, or programs that place undue burdens on the operation of the Software, or (c) interfere with or disrupt the integrity or performance of the Software or data contained therein. The use of the Software will be subject to any other restrictions (such as number of users, features, or duration of use) agreed to by the parties or as set forth in the Subscription Agreement.

3. SECURITY. Customer acknowledges that the information available through the LN Services may include personally identifiable information and it is Customer's obligation to keep all such accessed information confidential and secure. Accordingly, Customer shall (a) restrict access to LN Services to those employees who have a need to know as part of their official duties; (b) ensure that none of its employees shall (i) obtain and/or use any information from the LN Services for personal reasons, or (ii) transfer any information received through the LN Services to any party except as permitted hereunder; (c) keep all user identification numbers, and related passwords, or other security measures (collectively, "**User IDs**") confidential and prohibit the sharing of User IDs; (d) immediately deactivate the User ID of any employee who no longer has a need to know, or for terminated employees on or prior to the date of termination; (e) in addition to any obligations under Paragraph 2, take all commercially reasonable measures to prevent unauthorized access to, or use of, the LN Services or data received therefrom, whether the same is in electronic form or hard copy, by any person or entity; (f) maintain and enforce data destruction procedures to protect the security and confidentiality of all information obtained through LN Services as it is being disposed; (g) purge all information received through the LN Services within ninety (90) days of initial receipt; provided that Customer may extend such period if and solely to the extent such information is retained thereafter in archival form to provide documentary support required for Customer's legal or regulatory compliance efforts; (h) be capable of receiving the LN Services where the same are provided utilizing "**secure socket layer**," or such other means of secure transmission as is deemed reasonable by LN; (i) not access and/or use the LN Services via mechanical, programmatic, robotic, scripted or other automated search means, other than through batch or machine-to-machine applications approved by LN; (j) take all steps to protect their networks and computer environments, or those used to access the LN Services, from compromise; (k) on at least a quarterly basis, review searches performed by its User IDs to ensure that such searches were performed for a legitimate business purpose and in compliance with all terms and conditions herein; and (l) maintain policies and procedures to prevent unauthorized use of User IDs and the LN Services. Customer will immediately notify LN, by written notification to the LN Information Assurance and Data Protection Organization at 1000 Alderman Drive, Alpharetta, Georgia 30005 and by email (security.investigations@lexisnexis.com) and by phone (1-888-872-5375), if Customer suspects, has reason to believe or confirms that a User ID or the LN Services (or data derived directly or indirectly therefrom) is or has been lost, stolen, compromised, misused or used, accessed or acquired in an unauthorized manner or by any unauthorized person, or for any purpose contrary to the terms and conditions herein. To the extent permitted under applicable law, Customer shall remain solely liable for all costs associated therewith and shall further reimburse LN for any expenses it incurs due to Customer's failure to prevent such impermissible use or access of User IDs and/or the LN Services, or any actions required as a result thereof. Furthermore, in the event that the LN Services provided to the Customer include personally identifiable information (including, but not limited to, social security numbers, driver's license numbers or dates of birth), the following shall apply: Customer acknowledges that, upon unauthorized acquisition or access of or to such personally identifiable information, including but not limited to that which is due to use by an unauthorized person or due to unauthorized use (a "**Security Event**"), Customer shall, in compliance with law, notify the individuals whose information was potentially accessed or acquired that a Security Event has occurred, and shall also notify any other parties (including but not limited to regulatory entities and credit reporting agencies) as may be required in LN's reasonable discretion. Customer agrees that such notification shall not reference LN or the product through which the data was provided, nor shall LN be otherwise identified or referenced in connection with the Security Event, without LN's express written consent. Customer shall be solely responsible for any other legal or regulatory obligations which may arise under applicable law in connection with such a Security Event and shall bear all costs associated with complying with legal and regulatory obligations in connection therewith. To the extent permitted under applicable law, Customer shall remain solely liable for claims that may arise from a Security Event, including, but not limited to, costs for litigation (including attorneys' fees), and reimbursement sought by individuals, including but not limited to, costs for credit monitoring or allegations of loss in connection with the Security Event. Customer shall provide samples of all proposed materials to notify consumers and any third parties, including regulatory

entities, to LN for review and approval prior to distribution. In the event of a Security Event, LN may, in its sole discretion, take immediate action, including suspension or termination of Customer's account, without further obligation or liability of any kind.

4. PERFORMANCE. LN will use commercially reasonable efforts to deliver the LN Services requested by Customer and to compile information gathered from selected public records and other sources used in the provision of the LN Services; provided, however, that the Customer accepts all information "**AS IS**". Customer acknowledges and agrees that LN obtains its data from third party sources, which may or may not be completely thorough and accurate, and that Customer shall not rely on LN for the accuracy or completeness of information supplied through the LN Services. Without limiting the foregoing, the criminal record data that may be provided as part of the LN Services may include records that have been expunged, sealed, or otherwise have become inaccessible to the public since the date on which the data was last updated or collected. Customer understands that Customer may be restricted from accessing certain LN Services which may be otherwise available. LN reserves the right to add materials and features to, and to discontinue offering any of the materials and features that are currently a part of, the LN Services. In the event that LN discontinues a material portion of the materials and features that Customer regularly uses in the ordinary course of its business, and such materials and features are part of a flat fee subscription plan to which Customer has subscribed, LN will, at Customer's option, issue a prorated credit to Customer's account.

5. Reserved

6. INTELLECTUAL PROPERTY. Customer agrees that Customer shall not reproduce, retransmit, republish, or otherwise transfer for any commercial purposes the LN Services. Customer acknowledges that LN (and/or its third-party data providers) shall retain all right, title, and interest under applicable contractual, copyright, patent, trademark, and related laws in and to the LN Services and the information that they provide. Customer shall use such materials in a manner consistent with LN's interests and the terms and conditions herein, and shall promptly notify LN of any threatened or actual infringement of LN's rights.

7. PAYMENT OF FEES. Customer shall pay LN the fees described on the applicable Subscription Agreement. Customer shall be responsible for payment of the applicable fees for all services ordered by Customer or otherwise obtained through Customer's User IDs, whether or not such User ID is used by Customer or a third party, provided access to the User ID is not the result of use by a person formerly or presently employed by LN (and not employed by Customer at the time of the use) or who obtains the User ID by or through a break-in or unauthorized access of LN's offices, premises, records, or documents. Customer agrees that it may be electronically invoiced for those fees. Payments must be received by LN within accordance of Exhibit B of the MSA.

8. Reserved
9. Reserved
10. Reserved

11. GOVERNING LAW. In the event that Customer is a government agency, these Master Terms shall be governed by and construed in accordance with the state or federal law(s) applicable to such agency, irrespective of conflicts of law principles.

12. ASSIGNMENT. Neither these Master Terms nor the license granted herein may be assigned by Customer, in whole or in part, without the prior written consent of LN. The dissolution, merger, consolidation, reorganization, sale or other transfer of assets, properties, or controlling interest of twenty percent (20%) or more of Customer shall be deemed an assignment for the purposes of these Master Terms. Any assignment without the prior written consent of LN shall be void.

13. DISCLAIMER OF WARRANTIES. LN (SOLELY FOR PURPOSES OF DISCLAIMER OF WARRANTIES, AND LIMITATION ON LIABILITY, LN, ITS SUBSIDIARIES AND AFFILIATES, AND ITS DATA PROVIDERS ARE COLLECTIVELY REFERRED TO AS "LN") DOES NOT MAKE AND HEREBY DISCLAIMS ANY WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THE LN SERVICES. LN DOES NOT WARRANT THE CORRECTNESS, COMPLETENESS, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF THE LN SERVICES OR INFORMATION PROVIDED THEREIN. Due to the nature of public record information, the public records and commercially available data sources used in the LN Services may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. The LN Services are not the source of data, nor are they a comprehensive compilation of the data. Before relying on any data, it should be independently verified.

14. LIMITATION OF LIABILITY. Neither LN, nor its subsidiaries and affiliates, nor any third-party data provider shall be liable to Customer (or to any person claiming through Customer to whom Customer may have provided data from the LN Services) for any loss or injury arising out of or caused in whole or in part by use of the LN Services. If, notwithstanding the foregoing, liability can be imposed on LN, Customer agrees that LN's aggregate liability for any and all losses or injuries arising out of any act or omission of LN in connection with anything to be done or furnished under these Master Terms, regardless of the cause of the loss or injury, and regardless of the nature of the legal or equitable right claimed to have been violated, shall never exceed the amount of fees actually paid by Customer to LN under this Agreement during the six (6) month period preceding the event that gave rise to such loss or injury. Customer covenants and promises that it will not sue LN for an amount greater than such sum even if Customer and/or third parties were advised of the possibility of such damages and that it will not seek punitive damages in any suit against LN. IN NO EVENT SHALL LN BE LIABLE FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, HOWEVER ARISING, INCURRED BY CUSTOMER.

15. SURVIVAL OF AGREEMENT. Provisions hereof related to release of claims; use and protection of LN Services; payment for the LN Services; audit; LN's use and ownership of Customer's search inquiry data; disclaimer of warranties and other disclaimers; security; customer data and governing law shall survive any termination of the license to use the LN Services.

16. AUDIT. Customer understands and agrees that, in order to ensure compliance with the FCRA, GLBA, DPPA, other similar state or federal laws, regulations or rules, regulatory agency requirements of these Master Terms, LN's obligations under its contracts with its data providers, and LN's internal policies, LN may conduct periodic reviews and/or audits of Customer's use of the LN Services. Customer agrees to cooperate fully with any and all audits and to respond to any such audit inquiry within ten (10) business days, unless an expedited response is required. Violations discovered in any review and/or audit by LN will be subject to immediate action including, but not limited to, suspension or termination of the license to use the LN Services, reactivation fees, legal action, and/or referral to federal or state regulatory agencies.

17. EMPLOYEE TRAINING. Customer shall train new employees prior to allowing access to LN Services on Customer's obligations under these Master Terms, including, but not limited to, the licensing requirements and restrictions under Paragraph 2, the security requirements of Paragraph 3 and the privacy requirements in Paragraph 23. Customer shall conduct a similar review of its obligations under these Master Terms with existing employees who have access to LN Services no less than annually. Customer shall keep records of such training.

18. TAXES. The charges for all LN Services are exclusive of any state, local, or otherwise applicable sales, use, or similar taxes. If any such taxes are applicable, they shall be charged to Customer's account.

19. CUSTOMER INFORMATION. Customer certifies that Customer has not been the subject of any proceeding regarding any trust-related matter including, but not limited to, fraud, counterfeiting, identity theft and the like, and that Customer has not been the subject of any civil, criminal or regulatory matter that would create an enhanced security risk to LN, the LN Services or the data, including but not limited to, any matter involving potential violations of the GLBA, the DPPA, the FCRA, the Fair Debt Collection Practices Act ("**FDCPA**") (15 U.S.C. § 1692-1692p) or any other similar legal or regulatory guidelines. If any such matter has occurred, Customer shall attach a signed statement, along with all relevant supporting documentation, providing all details of this matter prior to execution of this Agreement. Customer shall notify LN immediately of any changes to the information on Customer's Application for the LN Services, and, if at any time Customer no longer meets LN's criteria for providing service, LN may terminate this agreement. Customer is required to promptly notify LN of a change in ownership of Customer, any change in the name of Customer, and/or any change in the physical address of Customer.

20. RELATIONSHIP OF PARTIES. None of the parties shall, at any time, represent that it is the authorized agent or representative of the other. LN's relationship to Customer in the performance of services pursuant to this Agreement is that of an independent contractor.

21. CHANGE IN AGREEMENT. By receipt of the LN Services, Customer agrees to, and shall comply with, changes to the restricted license granted to Customer hereunder. These terms may be changed only if such changes are dictated by governmental/regulatory directive or by a content licensor ("Directive"). If any changes are made to these terms by Directive, such changes will: (a) only be applied prospectively; and (b) not be specifically directed against the State Agency but will apply to all similarly situated LN customers."
The User Agency may terminate the Agreement or this Exhibit upon written notice to LN if any change to these Terms by Directive is unacceptable to the User Agency. Except as provided above, these Terms may not be supplemented, modified, changed or otherwise revised unless ninety (90) days' notice is provided to the State Contract Administrator and an amendment is signed by duly authorized representatives of both parties. Notices to Customer will be provided via written communication. All e-mail notifications shall be sent to the individual named in the Customer Administrator Contact Information section of the Application, unless stated otherwise. LN may, at any time, impose restrictions and/or prohibitions on the Customer's use of some or all of the LN Services. Customer understands that such restrictions or changes in access may be the result of a modification in LN policy, a modification of third-party agreements, a modification in industry standards, a Security Event or a change in law or regulation, or the interpretation thereof. Upon written notification by LN of such restrictions, Customer agrees to comply with such restrictions.

22. PRIVACY PRINCIPLES. With respect to personally identifiable information regarding consumers, the parties further agree as follows: LN has adopted the "LN Data Privacy Principles" ("**Principles**"), which may be modified when necessary to address new legal or legislative requirements or to include recent industry best practices recognizing the importance of appropriate privacy protections for consumer data, and Customer agrees that Customer (including its directors, officers, employees or agents) will comply with the Principles or Customer's own comparable privacy principles, policies, or practices. See the attached Data Privacy Principles. Notification of any such changes will be provided to the designated State Contract Administrator for this Agreement."

23. Reserved

24. FORCE MAJEURE. The parties will not incur any liability to each other or to any other party on account of any loss or damage resulting from any delay or failure to perform all or any part of these Master Terms (except for payment obligations) to the extent such delay or failure is caused, in whole or in part, by events, occurrences, or causes beyond the control, and without the negligence of, the parties. Such events, occurrences, or causes include, without limitation, acts of God, telecommunications outages, Internet outages,

power outages, any irregularity in the announcing or posting of updated data files by the applicable agency, strikes, lockouts, riots, acts of war, floods, earthquakes, fires, and explosions.

25. LN AFFILIATES. Customer understands that LN Services furnished under these Master Terms may be provided by LNRSFL, LNRSB and/or by one of their Affiliates. The specific LN entity furnishing the LN Services to Customer will be the sole LN entity satisfying all representations, warranties, covenants and obligations hereunder, as they pertain to the provision of such LN Services. Therefore, Customer hereby expressly acknowledges and agrees that it will seek fulfillment of any and all LN obligations only from the applicable LN entity and the other LN entities shall not be a guarantor of said LN entity's performance obligations hereunder.

26. CUSTOMER SUBSIDIARIES. LN may provide the LN Services to Customer's wholly owned subsidiaries ("**Subsidiaries**"), in LN' sole discretion, subject to the Subsidiaries' completion of LN's credentialing process and any applicable paperwork. Customer assumes full responsibility for such Subsidiaries.

27. MISCELLANEOUS. If any provision of these Master Terms or any exhibit shall be held by a court of competent jurisdiction to be contrary to law, invalid or otherwise unenforceable, such provision shall be changed and interpreted so as to best accomplish the objectives of the original provision to the fullest extent allowed by law, and in any event the remaining provisions of these Master Terms shall remain in full force and effect. The failure or delay by LN in exercising any right, power or remedy under this Agreement shall not operate as a waiver of any such right, power or remedy. The headings in these Master Terms are inserted for reference and convenience only and shall not enter into the interpretation hereof.

28. Reserved

Appendix I – LexisNexis Master Terms and Conditions (Document 2)

Risk Solutions Supplemental Terms & Conditions

NOTICE: THE FOLLOWING TERMS AND CONDITIONS APPLY TO YOUR USE OF THE LEXISNEXIS RISK SOLUTIONS GROUP PRODUCTS AND SERVICES.

The terms and conditions listed below govern use of the LexisNexis Risk Solutions Group services (the "LN Services") and materials available therein ("Materials"), provided by LexisNexis Risk Solutions FL Inc. and its affiliated companies (collectively, "LN"). The terms "Client", "Customer", "you", and "your" in uppercase or lowercase shall mean the entity (e.g., company, corporation, partnership, sole proprietor, etc.) or government agency entering into an agreement for the LN Services.

You agree to comply with the following terms and conditions:

TERMS AND CONDITIONS

I. **American Board of Medical Specialties ("ABMS") Data.**

If Customer is permitted to access ABMS Data from LN, Customer shall not use, nor permit others to use, ABMS Data for purposes of determining, monitoring, tracking, profiling or evaluating in any manner the patterns or frequency of physicians' prescriptions or medications, pharmaceuticals, controlled substances, or medical devices for use by their patients.

II. **BuildeRadius d/b/a BuildFax (Constructions Records and Building Permit Information)**

With respect to the construction records and building permit information in the LN Services, Client acknowledges and agrees that it is solely responsible for complying with, and agrees that its use of the LN Services, provided product, and any derivatives thereof, and any data provided to it by BuildFax or related to construction records and building permit information will comply with all applicable foreign, federal, state and local laws, regulations and ordinances, including , without limitation, the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.) the United States Freedom of Information, Open Record, Sunshine and other similar laws and regulations (collectively, the "applicable laws"). Client further acknowledges and agrees that in no event shall BuildFax be liable or responsible for Client's failure to comply with any applicable law, even if such non-compliance results from Client's use or reliance on the LN Services, provided product, any derivatives thereof, or any data provided by BuildFax. Without limiting the foregoing, Client acknowledges and understands that certain restrictions apply to the use of data obtained from federal, state and locals governments and agencies, and Client agrees to comply with such restrictions, including, without limitation, restrictions on a person's right to use such data for marketing purposes. Client acknowledges and agrees that BuildFax data relates solely to real property, and does not relate to any individual consumer, and that Client cannot identify a consumer based on a search of BuildFax's information.

III. **California Secretary of State**

THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY. CERTIFICATION CAN ONLY BE OBTAINED THROUGH THE SACRAMENTO, CALIFORNIA OFFICE OF THE SECRETARY OF STATE.

IV. **DPPA Regulated Information:**

It is unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of the Driver's Privacy Protection Act; and it shall be unlawful for any person to make false representation to obtain any personal information from an individual's motor vehicle record.

V. **Dun & Bradstreet**

Access to and use of the D&B database is subject to the Terms of Agreement between you, LN and Dun & Bradstreet, Inc. (D&B). By accessing the D&B Data (or the "Information"), you agree that you have authority to enter into the Terms of Agreement on behalf of your Company and that you have read the Terms of Agreement, understand them, and agree on behalf of yourself and your Company to be bound by them.

Terms of Agreement

A. All information which D&B furnished to you will be used by you solely as one factor in your business decisions and will not be used to determine an individual's eligibility for credit or insurance to be used primarily for personal, family or household purposes or to determine an individual's eligibility for employment. You also agree that the Information will not be used to engage in unfair or deceptive practices.

B. You agree that the information will not be reproduced, revealed or made available to anyone else, it being understood that the Information is licensed for your internal use only. To the extent permitted by law, you agree to indemnify, defend and hold harmless D&B from any claim or cause of action against D&B arising out of, or relating to, the use of the Information by individuals or entities which have not been authorized to have access to and/or use the Information.

C. You understand that you are the beneficiary of a contract between D&B and LN and that, under that contract, both D&B and LN have reserved certain rights which may result in the termination of your right to receive Information from D&B. In addition, D&B may terminate your receipt of the D&B data at any time if you breach any of its terms and conditions.

D. YOU ACKNOWLEDGE THAT D&B DOES NOT WARRANT OR GUARANTEE THE TIMELINESS, CURRENTNESS, ACCURACY, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE INFORMATION. YOU ALSO ACKNOWLEDGE THAT EVERY BUISNESS DECISION INVOLVES THE ASSUMPTION OF A RISK AND THAT D&B, IN FURNISHING THE INFORMATION TO YOU, DOES NOT AND WILL NOT UNDERWRITE THAT RISK, IN ANY MANNER WHATSOEVER. YOU THEREFORE, AGREE THAT D&B WILL NOT BE LIABLE FOR ANY LOSS, DAMAGE OR INJURY CAUSED IN WHOLE OR IN PART BY D&B'S NEGLIGENCE IN PROCURING, COMPILING, COLLECTING, INTERPRETING, REPORTING, COMMUNICATING OR DELIVERING THE INFORMATION.

E. YOU AGREE THAT D&B WILL NEVER BE LIABLE FOR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THEIR POSSIBILITY. YOU ALSO AGREE THAT D&B'S LIABILITY OF ANY AND ALL LOSSES, DAMAGES OR INJURIES WHICH YOU SUFFER OR INCUR ARISING OUT OF ANY ACTS OR OMISSIONS OF D&B IN CONNECTION WITH THE D&B DATA, REGARDLESS OF THE CAUSE OF THE LOSS, DAMAGE OR INJURY AND REGARDLESS OF THE NATURE OF THE LEGAL RIGHT CLAIMED TO HAVE BEEN VIOLATED, SHALL NEVER EXCEED $10,000.00 AND YOU COVENANT AND PROMISE THAT YOU WILL NOT SUE D&B FOR AN AMOUNT GREATER THAN THAT SUBJECT TO THIS SECTION E.

F. You acknowledge and agree that the copyright to the Information is and shall remain with D&B. You acknowledge that the Information, regardless of form or format, is proprietary to D&B and comprises: (a) works of original authorship, including compiled information containing D&B's selection, arrangement and coordination and expression of such information or pre-existing material it has created, gathered or assembled; (b) confidential or trade secret information; and (c) information that has been created, developed and maintained by D&B at great expense of time and money such that misappropriation or unauthorized use by others for commercial gain would unfairly and irreparably harm D&B. You shall not commit or permit any act or omission by your agents, employees or any third party that would impair D&B's proprietary and intellectual property rights in the Information. You agree to notify D&B

immediately upon obtaining any information regarding a threatened or actual infringement of D&B's rights.

G. These terms are in addition to those found in any LN service agreement. If there is a conflict between these terms and those found in any such service agreement, then these terms will apply. The agreement regarding your receipt and use of the D&B data shall be governed by the laws of the State of New Jersey, United States of America without giving effect to its conflicts of laws provisions. To the extent permitted by State law, any disputes arising hereunder must be filed and shall be venued in the United States District Court for the District of New Jersey or in the courts of the State of New Jersey and the parties hereby submit to the jurisdiction of such courts.

VI. **Experian Terms and Conditions located on pages 85 – 93 of this document.**

VII. **Georgia Secretary of State**

THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY; CERTIFICATION CAN ONLY BE OBTAINED THROUGH THE OFFICE OF THE GEORGIA SECRETARY OF STATE.

VIII. **RESERVED**

IX. **RESERVED**

X. **RESERVED.**

XI. **Michigan Corporations**

Provider, in producing the aforementioned CORPINFO disclaims any liability for the accuracy of any of the information. The CORPINFO is produced and sold for general information purposes only. Said CORPINFO is not to be construed as having the legal effect of a certified copy of any of the information appearing in the data file or an official certification of filing by Provider. When information contained within the CORPINFO is displayed on a video terminal, the following or a similarly worded statement will appear on either the menu screen or the beginning of each corporation record: "THIS DATA IS FOR INFORMATION PURPOSES ONLY. CERTIFICATION CAN ONLY BE OBTAI NED THROUGH THE MICHIGAN DEPARTMENT OF LICENSING AND REGULATORY AFFAIRS, CSCLB, CORPORATIONS DIVISION."

XII. **Michigan Department of Consumer and Industry Services, Corporation and Land Development Bureau**

THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY. CERTIFICATION CAN ONLY BE OBTAINED THROUGH THE MICHIGAN DEPARTMENT OF CONSUMER AND INDUSTRY SERVICES, CORPORATION DIVISION.

XIII. **Michigan Department of Energy, Labor and Economic Growth**

THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY. CERTIFICATION CAN ONLY BE OBTAINED THROUGH THE MICHIGAN DEPARTMENT OF ENERGY, LABOR AND ECONOMIC GROWTH, CORPORATE DIVISION.

XIV. **RESERVED.**

XV. **National Change of Address Database.**

LN is a licensee of the United States Postal Service's NCOALINK database ("NCOA Database"). The information contained in the NCOA Database is regulated by the Privacy Act of 1974 and may be used only to provide a mailing list correction service for lists that will be used for preparation of mailings. If Customer

receives all or a portion of the NCOA Database through the LN Services, Customer hereby certifies to LN that it will not use such information for any other purpose. Prior to obtaining or using information from the NCOA Database, Customer agrees to complete, execute and submit to LN the NCOA Processing Acknowledgement Form.

XVI. **New York State Department of State, Division of Corporations**

The information provided by the Department of State, Division of Corporations is not an official record of the Department of State or the State of New York. LN is not an employee or agent of the Department of State or the State of New York. The Department of State disclaims all warranties, express or implied, regarding the corporation's data.

XVII. **New York State Unified Court System**

The New York State Unified Court System ("UCS") does not warrant the comprehensiveness, completeness, accuracy or adequacy for any particular use or purpose of the information contained in its databases and expressly disclaims all other warranties, express or implied, as to any matter whatsoever. Neither the UCS, its courts, court-related agencies or its officers or employees shall be responsible for any loss or damage caused by the use of the information contained in any of its databases.

XVIII. **North Carolina Department of the Secretary of State**

State Of North Carolina - County Of Wake
(Corporations Data Files)

THIS DATA IS FOR INFORMATION PURPOSES ONLY. CERTIFICATION CAN ONLY BE OBTAINED THROUGH THE NORTH CAROLINA DEPARTMENT OF THE SECRETARY OF STATE.

XIX. **Pennsylvania Department of State, Corporation Bureau**

THIS DATA IS FOR INFORMATIONAL PURPOSES ONLY AND IS NOT AN OFFICIAL RECORD. CERTIFIED COPIES MAY BE OBTAINED FROM THE PENNSYLVANIA DEPARTMENT OF STATE.

XX. **Phone Numbers in General**

All phone numbers in the LN database must be used for legitimate and lawful purposes. It is customer's responsibility to comply with all rules and regulations related to the use and distribution of phone numbers, including landlines, and mobile phone numbers. All use of phone numbers from LN must be done in accordance with applicable law, including Do Not Call where appropriate.

XXI. **Private Investigator Use of the LN Services**

Investigators shall maintain up to date and current licenses so long as the Private Investigator is accessing the LN Services

XXII. **Property Records (Source A)**

You may not use any portion of these Materials to create, replace, supplement or enhance any title, legal, vesting, ownership or encumbrance report. You are prohibited from using the Materials to develop any models, scores, or analytics including any methodology that would seek to value, trend, appraise, insure, encumber, un-encumber or otherwise evaluate real property assets in any manner. You may not comingle, mix or combine Materials with real estate information that you obtain from other sources. You may not disclose or share with any third- party counts, layouts or statistical metrics relating to the Materials. The Materials shall not be used in connection with alternative insurance underwriting approaches or products without first obtaining written

permission. Further, the methodology that would see to value, trend, appraise, insure, encumber, un-encumber or otherwise evaluate real property assets in any manner.

XXIII. **Wisconsin Circuit Court Data Subscription**

1. If Subscriber publishes or releases WCCA Information relating to any criminal case to any other person in whole or in part, directly or as part of a compilation, Subscriber shall restate prominently the following advisory that appears on the WCCA website:
2. Notice to employers: It may be a violation of state law to discriminate against a job applicant because of an arrest or conviction record. Generally speaking, an employer may refuse to hire an applicant on the basis of a conviction only if the circumstances of the conviction substantially relate to the particular job. For more information, see Wisconsin Statute 111.335 and the Department of Workforce Development's Arrest and Conviction Records under the Law publication.

Data Privacy Principles (Document 3)

The LexisNexis Data Privacy Principles speak to the personally identifiable information, including sensitive personally identifiable information, collected, maintained, used or disseminated in connection with services offered by LexisNexis (meaning LexisNexis, a division of Reed Elsevier Inc., LexisNexis Risk Solutions Inc., and its or their affiliated companies) (hereinafter referred to individually or collectively as "LexisNexis")).

LexisNexis applies these Principles to our domestic U.S. products and services where appropriate. In addition, other uses or disclosures may occur as required by applicable law, such as the Fair Credit Reporting Act and its state analogues ("FCRA"), the Driver's Privacy Protection Act and its state analogues ("DPPA"), and the Gramm-Leach-Bliley Act ("GLB"). If the law requires or upon request of law enforcement, or, if necessary, to prevent fraud or to protect our company systems, these principles may not apply. LexisNexis also may revise our Data Privacy Principles by posting changes on its Web site. Changes will be made to the LN Data Privacy Principles when necessary to address new legal or legislative requirements or to include recent industry best practices. Notification of any such changes will be provided to the designated State Contract Administrator for this Agreement.

1. **SECURITY**
   Data security is a company imperative. LexisNexis strives to protect personally identifiable information that we maintain or disseminate, including through the use of appropriate administrative, physical, and technical safeguards.

2. **DISTRIBUTION OF PERSONALLY IDENTIFIABLE INFORMATION**
   LexisNexis strives to provide additional safeguards for sensitive personally identifiable information, such as Social Security numbers and driver's license numbers. LexisNexis strives to limit the availability and access to full Social Security Numbers ("SSNs"), Driver's License Numbers and State Identification Numbers. LexisNexis strives to protect the confidentiality of SSNs by limiting access to SSNs to certain legitimate and authorized users, such as: state, local and federal government entities; financial institutions; insurers; employers; creditors; debt collectors and other user types to which LexisNexis may decide to provide such access. A limited number of public records may contain SSNs that are already available to the public and, if such public records are accessed through LexisNexis services, our services may provide access to such SSNs. LexisNexis prohibits the unlawful disclosure of SSNs. LexisNexis also takes steps to limit the availability of Driver's License Numbers ("DLNs") and state identification card numbers.

3. **ACCURACY**
   LexisNexis strives to accurately report information in its products. LexisNexis also strives to accurately report information that it receives from its data sources. LexisNexis recognizes, however, that reporting errors may occur and offers individuals opportunities, where applicable, to dispute and correct information that we report as discussed further in Principle 9 on Access and Correction.

4. **PROTECTION OF SOCIAL SECURITY NUMBERS AND DRIVER'S LICENSE NUMBERS**
   LexisNexis strives to provide additional safeguards for sensitive personally identifiable information, such as Social Security numbers and driver's license numbers. LexisNexis strives to limit the availability and access to full Social Security Numbers ("SSNs"), Driver's License Numbers and State Identification Numbers. LexisNexis strives to protect the confidentiality of SSNs by limiting access to SSNs to certain legitimate and authorized users, such as: state, local and federal government entities; financial institutions; insurers; employers; creditors; debt collectors and other user types to which LexisNexis may decide to provide such access. A limited number of public records may contain SSNs that are already available to the public and, if such public records are accessed through LexisNexis services, our services may provide access to such SSNs. LexisNexis prohibits the unlawful disclosure of SSNs. LexisNexis also takes steps to limit the availability of Driver's License Numbers ("DLNs") and state identification card numbers.

5. **EDUCATION**
   LexisNexis strives to inform its employees, users and the general public about appropriate use of LexisNexis products and services. LexisNexis strives to inform its users and employees about:
   - Privacy and security issues associated with LexisNexis information products and services; and

- The responsible use of personally identifiable information.

LexisNexis strives to inform the public about:

- The responsible use of personally identifiable information;
- Measures LexisNexis has undertaken to enhance privacy; and choices available to individuals regarding information access and the ability to opt-out of certain products and services which utilize personally identifiable information.

6. REPUTABLE SOURCES

LexisNexis strives to acquire personally identifiable information from established, reputable sources in the government and private sectors. In support of this Principle, LexisNexis takes reasonable steps to assess the reputation and reliability of its private sector data sources before incorporating personally identifiable information from the source into its products and services. LexisNexis also strives to obtain assurances from its data suppliers that they have the legal right to license or sell the data to LexisNexis.

7. NOTICE

LexisNexis makes its Data Privacy Principles publicly known. LexisNexis publicly posts these Data Privacy Principles.

For additional information about the LexisNexis Data Privacy Principles, contact the LexisNexis Privacy Manager at 1-800-831-2578 or by mailing to:
Privacy Manager
LexisNexis
PO Box 933
Dayton, Ohio 45401

8. CHOICE

LexisNexis strives to allow individuals the opportunity to opt-out of the dissemination of personally identifiable information from certain LexisNexis owned databases used solely for marketing services. We also allow individuals to opt-out of LexisNexis' information products and services as required by law and permitted by LexisNexis policy.

9. ACCESS & CORRECTION

LexisNexis strives to provide individuals with a central point of contact regarding their questions about LexisNexis and its commitment to the responsible use of personally identifiable information. LexisNexis strives to inform individuals about the nature of the public records, nonpublic information, and publicly available information that LexisNexis makes available in its information products and services. LexisNexis also strives, whenever practicable, to provide individuals, upon request, with meaningful opportunities to review personally identifiable information we maintain about them. LexisNexis also strives, as appropriate and practicable, to provide opportunities for individuals to dispute and correct information by assisting them in identifying the potential information sources at which corrections should be made. LexisNexis strives to direct individuals to the government and private entities that collect and maintain public records and publicly available information to correct any claimed inaccuracies found in that data, and to direct individuals to consumer reporting agencies where such agency is the source of the information about the individual and where the individual seeks to correct claimed inaccuracies found in that data.

10. ACCOUNTABILITY

LexisNexis supports accountability of information industry standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. LexisNexis also supports industry oversight and active engagement with the privacy community. LexisNexis believes that strong privacy and information security protections are vital for an effective and trusted data industry.

11. ONLINE PRIVACY

LexisNexis strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply our Data Privacy Principles and evolving standards to the online environment.

12. IDENTITY THEFT

LexisNexis strives to prevent the acquisition of information from its products and services for improper purposes, such as identity theft. LexisNexis believes that it is important that individuals who may have had their sensitive personally identifiable information acquired by an unauthorized individual be notified as follows: Where a state law requires notice, LexisNexis complies with the law. In those states where notification laws do not exist, LexisNexis follows its Information Security Breach Response and Notification Policy, which provides that affected individuals will be notified when sensitive personally identifiable information owned or licensed by LexisNexis is acquired by an unauthorized individual and whenever LexisNexis has a reasonable basis to believe the breach has resulted in, or there is a significant risk that it will result in, identity theft to the consumer to whom the information relates.

13. COMPLIANCE

LexisNexis will obtain assessments from a qualified, objective, independent third-party, who uses procedures and standards generally accepted in the profession to assess LexisNexis' administrative, technical, and physical safeguards, as appropriate.

LexisNexis Risk Solutions Government Application (Document 4)

The information submitted on this Application will be used to determine the applicant's eligibility for accessing the services and products of LexisNexis Risk Solutions FL Inc. and its affiliates (hereinafter "LN"). To avoid delay, please provide all information requested. By submitting this Application, the applicant hereby authorizes LN to independently verify the information submitted and perform research about the individuals identified. Acceptance of this Application does not automatically create a business relationship between LN and the applicant. LN reserves the right to reject this Application with or without cause and to request additional information. Applicant acknowledges and understands that LN will only allow applicant access to the LN Services if applicant's credentials can be verified in accordance with LN's internal credentialing procedures.

Section I Agency Information please do not use abbreviations	
Full legal name of agency:	*Main phone number for address*:* *If this is a cell, additional documents may be required
If this application is for an additional account, Parent account number:	*Fax number:*
Physical Address where LN services will be accessed – P.O. Box/Mail Drops cannot be accepted (street, city, state, zip):	*Previous address if at the current address less than 6 months:*
Website address:	*External Agency IP Address (https://www.whatismyIP.com):*
External Agency IP Range – From:	*External Agency IP Range – To:*

Agency information:		
☐ Federal Government	☐ Federal Law Enforcement	☐ Local/Municipal Government
☐ State Government	☐ State Law Enforcement	☐ Local/Municipal Law Enforcement
☐ Other (please explain):		

Section II Administrator and Main Contact Information (for additional administrators, please provide additional sheets)	
Product Administrator or Main Contact (first & last name):	*Title:*
E-Mail Address:	*Admin IP Address:*
Required for local and municipal agencies:	
Administrator Home Address (street, city, state, zip):	*Administrator Date of Birth:*

Section III Billing Information	
Billing Contact (first & last name): *check here if same as Administrator* ☐	*Title:*
Billing Address (street, city, state, zip):	*Telephone:*
E-Mail Address:	*Sales Tax Exempt:* ☐No ☐Yes – please provide proof of exemption
Do you require a PO number on invoice:	
☐ No ☐ Yes If Yes, provide PO Number:	

Section IV Business to Business Vendor Reference	
Required for local and municipal agencies:	
Company Name:	Contact:
Business Address (street, city, state, zip):	Contact Phone Number:
E-mail Address:	Account Number (if applicable):

Section V Site Visits	
Site visits may be required to assure Applicant eligibility for LN products or services. By submitting this Application, Applicant agrees to authorize a site visit by LN or its approved third-party, and agrees to cooperate in its completion. If the contact for coordinating the site visit is not identified above as the Administrator, please provide the site visit contact's information below:	
Contact Name:	Contact Phone:
Contact Email Address:	

Signature	
I HEREBY CERTIFY that I am authorized to execute this Application on behalf of the Agency listed above and that I have direct knowledge of the facts stated above.	
Applicant Signature:	Date Signed:
Applicant Name:	Title:

FCRA PERMISSIBLE USE CERTIFICATION – GOVERNMENT (Document 5)

Customer (Agency) Name:
DBA:
Address:
City, State, Zip:
Contact Name: **Phone:**

REQUIRED Please describe your purpose of use:

SECTION 1. FCRA PERMISSIBLE PURPOSE

Customer, as a "User" of LexisNexis Risk Solutions Bureau LLC Consumer Reports, hereby certifies as follows:

1. The nature of Customer's business is: _____.

2. Customer's orders Consumer Reports from LN for the following purpose(s) under the Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq) ("**FCRA**") and such reports will not be used for any other purpose:

Please check **all** that apply (not all uses are available in every product):

- ☐ For the extension of credit to the consumer in connection with a credit transaction involving the consumer in accordance with 15 U.S.C. Sec. 1681b (a)(3)(A).
- ☐ For the review of an account of the consumer in connection with a credit transaction involving the consumer in accordance with 15 U.S.C. Sec. 1681b (a)(3)(A).
- ☐ For the collection of an account of the consumer in connection with a credit transaction involving the consumer in accordance with 15 U.S.C. Sec. 1681b (a)(3)(A).
- ☐ For use in connection with the underwriting of insurance involving the consumer in accordance with 15 U.S.C. Sec. 1681b (a)(3)(C).
- ☐ For use, 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 in accordance with 15 U.S.C. Sec.1681b (a)(3)(E).
- ☐ In connection with the assessment of the consumer's ability to pay for a medical care transaction initiated by the consumer, a legitimate business need pursuant to 15 U.S.C. Sec. 1681b (a)(3)(F)(i).
- ☐ In connection with a rental car transaction where the transaction is initiated by the consumer, a legitimate business need pursuant to 15 U.S.C. Sec. 1681b(a)(3)(F)(i).
- ☐ In connection with a demand deposit account or related new account opening transaction where the transaction is initiated by the consumer, a legitimate business need pursuant to 15 U.S.C. Sec. 1681b(a)(3)(F)(i).
- ☐ In response to a request by the head of a State or local child support enforcement agency (or a State or local government official authorized by the head of such an agency). In accordance with 15 U.S.C. Sec. 1681b (a)(4), Customer makes the following certifications:
  - (A) the consumer report is needed for the purpose of establishing an individual's capacity to make child support payments or determining the appropriate level of such payments;
  - (B) the paternity of the consumer for the child to which the obligation relates has been established or acknowledged by the consumer in accordance with State laws under which the obligation arises (if required by those laws);

(C) the Customer has provided at least 10 days' prior notice to the consumer whose report is requested, by certified or registered mail to the last known address of the consumer, that the report will be requested; and

(D) the consumer report will be kept confidential, will be used solely for a purpose described in subparagraph (A), and will not be used in connection with any other civil, administrative, or criminal proceeding, or for any other purpose.

☐ For use in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status in accordance with 15 U.S.C. Sec. 1681b (a)(3)(D).

☐ For use in making firm offers of credit in connection with credit transactions that are not initiated by the consumer in accordance with 15 U.S.C. Sec. 1681b(c) and as fully set forth in, and under the terms and conditions of, the Prescreening Services Addendum.

☐ With express written instructions of the consumer for reasons **other than** an employment purpose in accordance with FCRA Section 15 U.S.C. Sec. 1681b (a)(2).
If you have selected "with express written instructions of the consumer" above, please specify intended use: _____

3. The FCRA imposes criminal penalties – including a fine, up to two years in prison, or both – against anyone who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses, and other penalties for anyone who obtains such consumer information without a permissible purpose.

SECTION 2. QUALIFIED ACCESS

Customer may be able to obtain full social security numbers (nine (9) digits) and driver's license numbers (collectively, "QA Data"), if LN deems it appropriate, through some LN Services.

☐ Customer is **NOT** requesting access to QA Data

☐ Customer is requesting access to QA Data.

What department will be using QA Data? _____

SECTION 3. DEATH MASTER FILE

For access to Limited Access DMF Data only.

☐ No permissible purpose. Proceed to AUTHORIZATION AND ACCEPTANCE OF TERMS

I. Definitions. For purposes of this Certification, these terms are defined as follows:

a. DMF Agreement: The Limited Access Death Master File Non-federal Licensee Agreement for Use and Resale executed by LexisNexis Risk Data Retrieval Services LLC, on behalf of itself, its affiliates and subsidiaries, and its and their successors, with the federal government (NTIS, as below defined). The DMF Agreement form is found at www.lexisnexis.com/risk/DMFDocuments.

b. Certification Form: The Limited Access Death Master File Subscriber Certification Form executed by LexisNexis Risk Data Retrieval Services LLC, on behalf of itself, its affiliates and subsidiaries, and its and their successors, with the federal government (NTIS, as below defined). The Certification Form is found at www.lexisnexis.com/risk/DMFDocuments.

c. **DMF**: The federal Death Master File.
d. **NTIS:** National Technical Information Service, U.S. Department of Commerce
e. **Open Access DMF:** The DMF product made available through LN, which obtains the data from NTIS, and which does not include DMF with respect to any deceased individual at any time during the three-calendar-year period beginning on the date of the individual's death. Open Access DMF data should not be accessed pursuant to this Certification but should be accessed pursuant to a customer contract for such DMF data that is not Limited Access DMF.
f. **Limited Access DMF**: Limited Access DMF includes DMF data with respect to any deceased individual at any time during the three-calendar-year period beginning on the date of the individual's death. Limited Access DMF is made available through LN as a Certified Person, by NTIS. This Certification governs Customer's access to Limited Access DMF from LN (or the applicable LN affiliate), whether full or partial Limited Access DMF records or indicators of deceased status, and via any format, including online, XML feed, or in-house file processing through LN.

II. Certification.

Customer's access to the Limited Access DMF requires certification of purpose, as required by 15 CFR Part 1110 and section 1001 of Title 18, United States Code. Customer hereby certifies that it has the indicated permissible purpose(s) under part (a) of this Section II ("Certification") and that it meets the requirements of part (b) of this Section II:

(a) Such Customer has a legitimate fraud prevention interest, or has a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty, will use the Limited Access DMF only for such purpose(s), and specifies the basis for so certifying as (choose any applicable purposes that apply to Customer's use):

☐ **Legitimate Fraud Prevention Interest:** Customer has a legitimate fraud prevention interest to detect and prevent fraud and/or to confirm identities across its commercial business and/or government activities.

☐ **Legitimate Business Purpose Pursuant to a Law, Governmental Rule, Regulation, or Fiduciary Duty:** Customer has one or more of the purposes permitted under 42 USC 1306c including fraud prevention and ID verification purposes. Customer's specific purpose(s) for obtaining Limited Access DMF data under this Certification is:

☐ Fraud Prevention and identity verification purposes
☐ For uses permitted or required by law
☐ For uses permitted or required by governmental rules
☐ For uses permitted or required by regulation
☐ For uses necessary to fulfill or avoid violating fiduciary duties

and

(b) Customer has systems, facilities, and procedures in place to safeguard Limited Access DMF, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986, and

(c) Customer agrees to satisfy the requirements of such section 6103(p)(4) as if such section applied to Customer.

III. Flow-down Agreement Terms and Conditions

The Parties agree that the following terms and conditions are applicable to Recipient and ordering, access to, and use of Limited Access DMF:

1. **Compliance with Terms of Agreement and CFR.** Recipient of Limited Access DMF must comply with the terms of the Agreement and the requirements of 15 CFR Part 1110, as though set forth as a Subscriber therein, and Recipients may not further distribute the Limited Access DMF.
2. **Change in Status**. Should Recipient's status change such that it would no longer have a permissible purpose to access Limited Access DMF under this Addendum, Recipient agrees to immediately notify LN in writing in the manner and format required for notices under the Contract. Should Recipient cease to have access rights to Limited Access DMF, Recipient shall destroy all Limited Access DMF, and will certify to LN in writing that is has destroyed all such DMF.
3. **Security and Audit**. Recipient will at all times have security provisions in place to protect the Limited Access DMF from being visible, searchable, harvestable or in any way discoverable on the World Wide Web. Recipient understands that any successful attempt by any person to gain unauthorized access to or use of the Limited Access DMF provided by LN may result in immediate termination of Recipient's access and this Addendum. In addition, any successful attempt by any person to gain unauthorized access may under certain circumstances result in penalties as prescribed in 15 CFR § 1110.200 levied on Recipient and the person attempting such access. Recipient will take appropriate action to ensure that all persons accessing the Limited Access DMF it obtains from LN are aware of their potential liability for misuse or attempting to gain unauthorized access. Any such access or attempted access is a breach, or attempted breach, of security and Recipient must immediately report the same to NTIS at dmfcert@ntis.gov; and to LN by written notification to the LN Information Assurance and Data Protection Organization at 1000 Alderman Drive, Alpharetta, Georgia 30005 and by email (security.investigations@lexisnexis.com) and by phone (1-888-872-5375). Recipient agrees to be subject to audit by LN and/or NTIS to determine Recipient's compliance with the requirements of this Addendum, the Agreement, and 15 CFR Part 1110. Recipient agrees to retain a list of all employees, contractors, and subcontractors to which it provides Limited Access DMF and to make that list available to NTIS and/or LN as part of any audits conducted hereunder. Recipient will not resell or otherwise redistribute the Limited Access DMF.
4. **Penalties.** Recipient acknowledges that failure to comply with the provisions of paragraph (3) of the Certification Form may subject Recipient to penalties under 15 CFR § 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year, or potentially uncapped for willful disclosure.
5. **Law, Dispute Resolution, and Forum.** Recipient acknowledges that this Addendum is governed by the terms of federal law. Recipient acknowledges that the terms of Section 14 of the Agreement govern disagreement handling, and, without limitation to the foregoing, that jurisdiction is federal court.
6. **Liability.** The U.S. Government/NTIS and LN (a) make no warranty, express or implied, with respect to information provided under the Agreement, including but not limited to, implied warranties of merchantability and fitness for any particular use; (b) assume no liability for any direct, indirect or consequential damages flowing from any use of any part of the Limited Access DMF, including infringement of third party intellectual property rights; and (c) assume no liability for any errors or

omissions in Limited Access DMF. The Limited Access DMF does have inaccuracies and NTIS and the Social Security Administration (SSA), which provides the DMF to NTIS, and LN, do not guarantee the accuracy of the Limited Access DMF. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person in the Limited Access DMF is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the Limited Access DMF. Recipient specifically acknowledges the terms of Attachment B to the Agreement, which terms apply to Recipient.

7. **Indemnification.** To the extent permitted by law, Recipient shall indemnify and hold harmless LN and NTIS and the Department of Commerce from all claims, liabilities, demands, damages, expenses, and losses arising from or in connection with Recipient's, Recipient's employees', contractors', or subcontractors' use of the Limited Access DMF. This provision will include any and all claims or liability arising from intellectual property rights.
8. **Survival**. Provisions hereof related to indemnification, use and protection of Limited Access DMF, audit, disclaimer of warranties, and governing law shall survive termination of this Addendum.
9. **Conflict of Terms.** Recipient acknowledges that the terms of this Addendum, in the event of conflict with the terms of the Contract, apply in addition to, and not in lieu of, such Contract terms, with respect to the Limited Access DMF only.

AUTHORIZATION AND ACCEPTANCE OF TERMS

I HEREBY CERTIFY that I have direct knowledge of the facts stated above and that I am authorized to execute this Certification on behalf of the Customer listed above.

CUSTOMER:

Signature:

Print:

Title:

Dated: (mm/dd/yy)

NON-FCRA PERMISSIBLE USE CERTIFICATION – GOVERNMENT (Document 6)

Customer (Agency) Name:
DBA:
Address:
City, State, Zip:
Contact Name: **Phone:**

REQUIRED Please describe your purpose of use:

Definitions. Gramm-Leach-Bliley Act, (15 U.S.C. § 6801, et seq.) and related state laws (collectively, the "GLBA")
Drivers Privacy Protection Act, (18 U.S.C. § 2721 et seq.) and related state laws (collectively, the "DPPA")

Law Enforcement Agencies Only: Review and, if appropriate, certify to the following: Customer represents and warrants that it will use the LN Services solely for law enforcement purposes, which comply with applicable privacy laws including, but not limited to the GLBA and the DPPA. To certify, check here: ☐
Proceed to SECTION 3. QUALIFIED ACCESS

SECTION 1. GLBA EXCEPTION/PERMISSIBLE PURPOSE - NOT APPLICABLE TO LAW ENFORCEMENT

Some LN Services use and/or display nonpublic personal information that is governed by the privacy provisions of the GLBA. Customer certifies it has the permissible purposes under the GLBA to use and/or obtain such information, as marked below, and Customer further certifies it will use such information obtained from LN Services only for such purpose(s) selected below or, if applicable, for the purpose(s) indicated by Customer electronically while using the LN Services, which purpose(s) will apply to searches performed during such electronic session:

☐ No applicable GLBA exception/permissible use. Proceed to SECTION 2. DPPA PERMISSIBLE USES

(At least one (1) must be checked to be permitted access to GLBA data)

☐	As necessary to effect, administer, or enforce a transaction requested or authorized by the consumer.
☐	As necessary to effect, administer, or enforce a transaction requested or authorized by the consumer by verifying the identification information contained in applications.
☐	To protect against or prevent actual or potential fraud, unauthorized transactions, claims or other liability.
☐	In required institutional risk control programs.
☐	In resolving consumer disputes or inquiries.
☐	Use by persons, or their representatives, holding a legal or beneficial interest relating to the consumer.
☐	Use by persons acting in a fiduciary or representative capacity on behalf of the consumer.
☐	In complying with federal, state, or local laws, rules, and other applicable legal requirements.
☐	To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies (including a Federal functional regulator, the Secretary of Treasury, a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety.

SECTION 2. DPPA PERMISSIBLE USES - NOT APPLICABLE TO LAW ENFORCEMENT

Some LN Services use and/or display personal information, the use of which is governed by the DPPA. Customer certifies it has a permissible use under the DPPA to use and/or obtain such information and Customer further certifies it will use such information obtained from LN Services only for one (1) or more of the purposes selected below or for the purpose(s) indicated by Customer electronically while using the LN Services, which purpose(s) will apply to searches performed during such electronic session:

☐ No permissible use. Proceed to SECTION 3. QUALIFIED ACCESS

(At least one (1) must be checked to be permitted access to DPPA data)

☐	For use in connection with any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a federal, state, or local court.
☐	For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only— **(A)** to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and **(B)** if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
☐	Use by a government agency, but only in carrying out its functions.
☐	Use by any person acting on behalf of a government agency, but only in carrying out the agency's functions.
☐	Use by an insurer (or its agent) in connection with claims investigation activities or antifraud activities.
☐	In connection with motor vehicle safety or theft, or driver safety (except by or for a motor vehicle manufacturer).
☐	Use by an employer or its agents or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under Chapter 313 of Title 49 of the United States Code.
☐	For use in providing notice to the owners of towed or impounded vehicles.
☐	For use in connection with the operation of private toll transportation facilities.

With regard to the information that is subject to the DPPA, some state laws' permissible uses may vary from the permissible uses identified above. In such cases, some state information may not be available under each permissible use listed above and/or Customer may be asked to certify to a permissible use permitted by applicable state law to obtain information from a specific state.

Customer agrees and certifies it will use the information described above only in accordance with the permissible uses selected above or those selected subsequently in connection with a specific information request.

SECTION 3. QUALIFIED ACCESS

Certain users ("Authorized Users") may be able to obtain full social security numbers (nine (9) digits) and driver's license numbers (collectively, "QA Data"), when appropriate, through some LN Services. Only those users that are within the Authorized User List below, and that use QA Data for an Authorized Use identified below, may

qualify. To potentially qualify as an Authorized User, Customer must certify that its business is within the Authorized User List below and its use of QA Data is within the Authorized Use List below.

☐ Customer is **NOT** requesting access to QA Data. Proceed to SECTION 4. DEATH MASTER FILE

☐ Customer is requesting access to QA Data. Complete the sections below.

What department will be using QA Data? _____

SOCIAL SECURITY NUMBERS

☐ Not an authorized user. Proceed to DRIVER'S LICENSE NUMBERS

1. AUTHORIZED USER (At least one (1) must be checked to receive Social Security Numbers)

☐	Federal, state or local government agency with law enforcement responsibilities.
☐	Special investigative unit, subrogation department and claims department of a private or public insurance company for the purposes of detecting, investigating or preventing fraud.
☐	Financial institution for the purposes of (a) detecting, investigating or preventing fraud, (b) compliance with federal or state laws or regulations, (c) collecting debt on their own behalf, and (d) such other uses as shall be appropriate and lawful.
☐	Collection department of a creditor.
☐	Collection company acting on behalf of a creditor or on its own behalf.
☐	Other public or private entity for the purpose of detecting, investigating or preventing fraud. Describe your business:

2. AUTHORIZED USE (At least one (1) must be checked to receive Social Security Numbers)

☐	Location of suspects or criminals.
☐	Location of non-custodial parents allegedly owing child support and ex-spouses allegedly owing spousal support.
☐	Location of individuals alleged to have failed to pay taxes or other lawful debts.
☐	Identity verification.
☐	Other uses similar to those described above. Describe your use:

By selecting above, the Customer certifies that it is an Authorized User, and that it will use Social Security Numbers only for the purpose(s) it designated on the Authorized Use List and for no other purpose(s).

DRIVER'S LICENSE NUMBERS

☐ Not an authorized user. Proceed to SECTION 4. DEATH MASTER FILE

1. AUTHORIZED USER (At least one (1) must be checked to receive Driver's License Numbers)

☐	Federal, state or local government agency with law enforcement responsibilities.
☐	Special investigative unit, subrogation department and claims department of a private or public insurance company for the purposes of detecting, investigating or preventing fraud.

☐	Financial institution for the purposes of (a) detecting, investigating or preventing fraud, (b) compliance with federal or state laws or regulations, (c) collecting debt on their own behalf, and (d) such other uses as shall be appropriate and lawful.
☐	Collection department of a creditor.
☐	Collection company acting on behalf of a creditor or on its own behalf.
☐	Other public or private entity for the purpose of detecting, investigating or preventing fraud. Describe your business:

2. AUTHORIZED USE (At least one (1) must be checked to receive Driver's License Numbers)

☐	Location of suspects or criminals.
☐	Location of non-custodial parents allegedly owing child support and ex-spouses allegedly owing spousal support.
☐	Location of individuals alleged to have failed to pay taxes or other lawful debts.
☐	Identity verification.
☐	Other uses similar to those described above. Describe your use:

By selecting above, the Customer certifies that it is an Authorized User, and that it will use Driver's License Numbers only for the purpose(s) it designated on the Authorized Use List and for no other purpose(s).

SECTION 4. DEATH MASTER FILE

For access to Limited Access DMF Data only.

☐ No permissible purpose. Proceed to AUTHORIZATION AND ACCEPTANCE OF TERMS

I. **Definitions.** For purposes of this Certification, these terms are defined as follows:

a. **DMF Agreement:** The Limited Access Death Master File Non-federal Licensee Agreement for Use and Resale executed by LexisNexis Risk Data Retrieval Services LLC, on behalf of itself, its affiliates and subsidiaries, and its and their successors, with the federal government (NTIS, as below defined). The DMF Agreement form is found at www.lexisnexis.com/risk/DMFDocuments.

b. **Certification Form:** The Limited Access Death Master File Subscriber Certification Form executed by LexisNexis Risk Data Retrieval Services LLC, on behalf of itself, its affiliates and subsidiaries, and its and their successors, with the federal government (NTIS, as below defined). The Certification Form is found at www.lexisnexis.com/risk/DMFDocuments.

c. **DMF**: The federal Death Master File.

d. **NTIS:** National Technical Information Service, U.S. Department of Commerce

e. **Open Access DMF:** The DMF product made available through LN, which obtains the data from NTIS, and which does not include DMF with respect to any deceased individual at any time during the three-calendar-year period beginning on the date of the individual's death. Open Access DMF data should not be accessed pursuant to this Certification but should be accessed pursuant to a customer contract for such DMF data that is not Limited Access DMF.

f. **Limited Access DMF**: Limited Access DMF includes DMF data with respect to any deceased individual at any time during the three-calendar-year period beginning on the date of the individual's death. Limited Access DMF is made available through LN as a Certified Person, by NTIS. This Certification governs Customer's access to Limited Access DMF from LN (or the applicable LN affiliate), whether full or partial Limited Access DMF records or indicators of deceased status, and via any format, including online, XML feed, or in-house file processing through LN.

II. Certification.

Customer's access to the Limited Access DMF requires certification of purpose, as required by 15 CFR Part 1110 and section 1001 of Title 18, United States Code. Customer hereby certifies that it has the indicated permissible purpose(s) under part (a) of this Section II ("Certification") and that it meets the requirements of part (b) of this Section II:

(a) Such Customer has a legitimate fraud prevention interest, or has a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty, will use the Limited Access DMF only for such purpose(s), and specifies the basis for so certifying as (choose any applicable purposes that apply to Customer's use):

☐ **Legitimate Fraud Prevention Interest:** Customer has a legitimate fraud prevention interest to detect and prevent fraud and/or to confirm identities across its commercial business and/or government activities.

☐ **Legitimate Business Purpose Pursuant to a Law, Governmental Rule, Regulation, or Fiduciary Duty:** Customer has one or more of the purposes permitted under 42 USC 1306c including fraud prevention and ID verification purposes. Customer's specific purpose(s) for obtaining Limited Access DMF data under this Certification is:

- ☐ Fraud Prevention and identity verification purposes
- ☐ For uses permitted or required by law
- ☐ For uses permitted or required by governmental rules
- ☐ For uses permitted or required by regulation
- ☐ For uses necessary to fulfill or avoid violating fiduciary duties

and

(b) Customer has systems, facilities, and procedures in place to safeguard Limited Access DMF, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986, and

(c) Customer agrees to satisfy the requirements of such section 6103(p)(4) as if such section applied to Customer.

III. Flow-down Agreement Terms and Conditions

The Parties agree that the following terms and conditions are applicable to Recipient and ordering, access to, and use of Limited Access DMF:

1. **Compliance with Terms of Agreement and CFR.** Recipient of Limited Access DMF must comply with the terms of the Agreement and the requirements of 15 CFR Part 1110, as though set forth as a Subscriber therein, and Recipients may not further distribute the Limited Access DMF.

2. **Change in Status**. Should Recipient's status change such that it would no longer have a permissible purpose to access Limited Access DMF under this Addendum, Recipient agrees to immediately notify LN in writing in the manner and format required for notices under the Contract. Should Recipient cease to have access rights to Limited Access DMF, Recipient shall destroy all Limited Access DMF, and will certify to LN in writing that is has destroyed all such DMF.
3. **Security and Audit**. Recipient will at all times have security provisions in place to protect the Limited Access DMF from being visible, searchable, harvestable or in any way discoverable on the World Wide Web. Recipient understands that any successful attempt by any person to gain unauthorized access to or use of the Limited Access DMF provided by LN may result in immediate termination of Recipient's access and this Addendum. In addition, any successful attempt by any person to gain unauthorized access may under certain circumstances result in penalties as prescribed in 15 CFR § 1110.200 levied on Recipient and the person attempting such access. Recipient will take appropriate action to ensure that all persons accessing the Limited Access DMF it obtains from LN are aware of their potential liability for misuse or attempting to gain unauthorized access. Any such access or attempted access is a breach, or attempted breach, of security and Recipient must immediately report the same to NTIS at dmfcert@ntis.gov; and to LN by written notification to the LN Information Assurance and Data Protection Organization at 1000 Alderman Drive, Alpharetta, Georgia 30005 and by email (security.investigations@lexisnexis.com) and by phone (1-888-872-5375). Recipient agrees to be subject to audit by LN and/or NTIS to determine Recipient's compliance with the requirements of this Addendum, the Agreement, and 15 CFR Part 1110. Recipient agrees to retain a list of all employees, contractors, and subcontractors to which it provides Limited Access DMF and to make that list available to NTIS and/or LN as part of any audits conducted hereunder. Recipient will not resell or otherwise redistribute the Limited Access DMF.
4. **Penalties.** Recipient acknowledges that failure to comply with the provisions of paragraph (3) of the Certification Form may subject Recipient to penalties under 15 CFR § 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year, or potentially uncapped for willful disclosure.
5. **Law, Dispute Resolution, and Forum.** Recipient acknowledges that this Addendum is governed by the terms of federal law. Recipient acknowledges that the terms of Section 14 of the Agreement govern disagreement handling, and, without limitation to the foregoing, that jurisdiction is federal court.
6. **Liability.** The U.S. Government/NTIS and LN (a) make no warranty, express or implied, with respect to information provided under the Agreement, including but not limited to, implied warranties of merchantability and fitness for any particular use; (b) assume no liability for any direct, indirect or consequential damages flowing from any use of any part of the Limited Access DMF, including infringement of third party intellectual property rights; and (c) assume no liability for any errors or omissions in Limited Access DMF. The Limited Access DMF does have inaccuracies and NTIS and the Social Security Administration (SSA), which provides the DMF to NTIS, and LN, do not guarantee the accuracy of the Limited Access DMF. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person in the Limited Access DMF is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the Limited Access DMF. Recipient specifically acknowledges the terms of Attachment B to the Agreement, which terms apply to Recipient.

7. **Indemnification.** To the extent permitted by law, Recipient shall indemnify and hold harmless LN and NTIS and the Department of Commerce from all claims, liabilities, demands, damages, expenses, and losses arising from or in connection with Recipient's, Recipient's employees', contractors', or subcontractors' use of the Limited Access DMF. This provision will include any and all claims or liability arising from intellectual property rights.
8. **Survival**. Provisions hereof related to indemnification, use and protection of Limited Access DMF, audit, disclaimer of warranties, and governing law shall survive termination of this Addendum.
9. **Conflict of Terms.** Recipient acknowledges that the terms of this Addendum, in the event of conflict with the terms of the Contract, apply in addition to, and not in lieu of, such Contract terms, with respect to the Limited Access DMF only.

AUTHORIZATION AND ACCEPTANCE OF TERMS

I HEREBY CERTIFY that I am authorized to execute this Non-FCRA Addendum on behalf of the Customer listed above.

CUSTOMER:

Signature:

Print:

Title:

Dated: (mm/dd/yy)

FCRA Addendum to the LexisNexis Master Terms and Conditions (form LNMTC) (Document 7)

This FCRA Addendum (the "**FCRA Addendum**") is entered into as of (the "**Effective Date**"), by and between **LexisNexis Risk Solutions Bureau LLC and its Affiliates** (hereinafter, "**LNRSB**"), with its principal place of business located at 1000 Alderman Drive, Alpharetta, Georgia 30005 and (hereinafter, "**Customer**"), with its principal place of business located at , each individually referred to as the "**Party**" and collectively as the "**Parties**."

WHEREAS, Customer has executed the LexisNexis Master Terms and Conditions (form LNMTC) (the "**Master Terms**") for the LN Services (as defined in the Master Terms); and

WHEREAS, the Parties wish to add certain terms and conditions to the Master Terms to govern the provision of FCRA LN Services (as defined below).

NOW, **THEREFORE**, LNRSB and Customer agree to be mutually bound by the additional terms and conditions of this FCRA Addendum, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, do hereby agree as follows:

1. **Fair Credit Reporting Act Obligations**. Customer certifies that when using the LN Services provided under this FCRA Addendum (as defined in the Master Terms) as an FCRA service (the "**FCRA LN Services**"), it will comply with all applicable provisions of the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("**FCRA**") and all other applicable federal, state and local legislation, regulations and rules. Without limiting the generality of the foregoing, Customer certifies that Customer will comply with all applicable provisions of the California Credit Reporting Agencies Act and any related regulations. In addition, Customer certifies it has a permissible purpose under the FCRA for obtaining a Consumer Report as provided by the Customer in a separate certification, and will re-certify such permissible purpose to LNRSB upon request. Customer acknowledges that LNRSB has provided the "Notice to Users of Consumer Reports", attached hereto as Attachment A, which informs users of consumer reports of their legal obligations under the FCRA.

2. **General.** Customer and LNRSB agree that: (i) capitalized terms used herein but not otherwise defined herein shall have the meanings ascribed to them in the Master Terms; (ii) this FCRA Addendum modifies and amends only those specific terms of the Master Terms expressly referenced herein; and (iii) all terms of the Master Terms are hereby restated as if written herein, shall remain in full force and effect, and shall constitute the legal valid, binding and enforceable obligations of the parties.

AUTHORIZATION AND ACCEPTANCE OF TERMS

I HEREBY CERTIFY that I am authorized to execute this FCRA Addendum on behalf of the Customer listed above.

CUSTOMER:

Signature:

Print:

Title:

Dated: (mm/dd/yy)

Attachment A – FCRA Addendum

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

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

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

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

I. OBLIGATIONS OF ALL USERS OF CONSUMER REPORTS

A. Users Must Have a Permissible Purpose

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

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

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

B. Users Must Provide Certifications

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

C. Users Must Notify Consumers When Adverse Actions Are Taken

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

1. Adverse Actions Based on Information Obtained From a CRA

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

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

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

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

3. Adverse Actions Based on Information Obtained From Affiliates

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

30 days after receiving the request. If consumer report information is shared among affiliates and then used for an adverse action, the user must make an adverse action disclosure as set forth in I.C.1 above.

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

When a consumer has placed a fraud alert, including one relating to identity theft, or an active duty military alert with a nationwide consumer reporting agency as defined in Section 603(p) and resellers, Section 605A(h) imposes limitations on users of reports obtained from the consumer reporting agency in certain circumstances, including the establishment of a new credit plan and the issuance of additional credit cards. For initial fraud alerts and active duty alerts, the user must have reasonable policies and procedures in place to form a belief that the user knows the identity of the applicant or contact the consumer at a telephone number specified by the consumer; in the case of extended fraud alerts, the user must contact the consumer in accordance with the contact information provided in the consumer's alert.

E. Users Have Obligations When Notified of an Address Discrepancy

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

F. Users Have Obligations When Disposing of Records

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

II. CREDITORS MUST MAKE ADDITIONAL DISCLOSURES

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

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

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

A. Employment Other Than in the Trucking Industry

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

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

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

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

B. Employment in the Trucking Industry

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

IV. OBLIGATIONS WHEN INVESTIGATIVE CONSUMER REPORTS ARE USED

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

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

V. SPECIAL PROCEDURES FOR EMPLOYEE INVESTIGATIONS

Section 603(x) provides special procedures for investigations of suspected misconduct by an employee or for compliance with Federal, state or local laws and regulations or the rules of a self-regulatory organization, and compliance with written policies of the employer. These investigations are not treated as consumer reports so long as the employer or its agent complies with the procedures set forth in Section 603(x), and a summary describing the nature and scope of the inquiry is made to the employee if an adverse action is taken based on the investigation.

VI. OBLIGATIONS OF USERS OF MEDICAL INFORMATION

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

VII. OBLIGATIONS OF USERS OF "PRESCREENED" LISTS

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

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

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

VIII. VIII. OBLIGATIONS OF RESELLERS

A. Disclosure and Certification Requirements

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

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

B. Reinvestigations by Resellers

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

C. Fraud Alerts and Resellers

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

IX. LIABILITY FOR VIOLATIONS OF THE FCRA

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

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

Citations for FCRA sections in the U.S. Code, 15 U.S.C. § 1618 et seq.:

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

Non-FCRA Addendum to the LexisNexis Master Terms and Conditions (form LNMTC) (Document 8)

This Non-FCRA Addendum (the "**Non-FCRA Addendum**") is entered into as of (the "**Effective Date**"), by and between **LexisNexis Risk Solutions FL Inc. and its Affiliates** (hereinafter, "**LNRSFL**"), with its principal place of business located at 1000 Alderman Drive, Alpharetta, Georgia 30005 and (hereinafter, "**Customer**"), with its principal place of business located at , each individually referred to as the "**Party**" and collectively as the "**Parties**."

WHEREAS, Customer has executed the LexisNexis Master Terms and Conditions (form LNMTC) (the "**Master Terms**") for the LN Services (as defined in the Master Terms); and

WHEREAS, the Parties wish to add certain terms and conditions to the Master Terms to govern the provision of Non-FCRA LN Services (as defined below).

NOW, **THEREFORE**, LNRSFL and Customer agree to be mutually bound by the additional terms and conditions of this Non-FCRA Addendum, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, do hereby agree as follows:

1. **Non-FCRA Use Restrictions**. The LN Services provided pursuant to this Non-FCRA Addendum (as defined in the Master Terms) as Non-FCRA are not provided by "consumer reporting agencies," as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("**FCRA**") and do not constitute "consumer reports," as that term is defined in the FCRA (the "**Non-FCRA LN Services**"). Accordingly, the Non-FCRA LN Services may not be used in whole or in part as a factor in determining eligibility for credit, insurance, employment or another purpose in connection with which a consumer report may be used under the FCRA. Further, (A) Customer certifies that it will not use any of the information it receives through the Non-FCRA LN Services to determine, in whole or in part an individual's eligibility for any of the following products, services or transactions: (1) credit or insurance to be used primarily for personal, family or household purposes; (2) employment purposes; (3) a license or other benefit granted by a government agency; or (4) any other product, service or transaction in connection with which a consumer report may be used under the FCRA or any similar state statute, including without limitation apartment rental, check-cashing, or the opening of a deposit or transaction account; (B) by way of clarification, without limiting the foregoing, Customer may use, except as otherwise prohibited or limited by this Non-FCRA Addendum, information received through the Non-FCRA LN Services for the following purposes: (1) to verify or authenticate an individual's identity; (2) to prevent or detect fraud or other unlawful activity; (3) to locate an individual; (4) to review the status of a legal proceeding; (5) to collect a debt, provided that such debt collection does not constitute in whole or in part, a determination of an individual consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; or (6) to determine whether to buy or sell consumer debt or a portfolio of consumer debt in a commercial secondary market transaction, provided that such determination does not constitute in whole or in part, a determination of an individual consumer's eligibility for credit or insurance to be used primarily for personal, family or household purposes; (C) specifically, if Customer is using the Non-FCRA LN Services in connection with collection of a consumer debt on its own behalf, or on behalf of a third-party, Customer shall not use the Non-FCRA LN Services: (1) to revoke consumer credit; (2) to accelerate, set or change repayment terms; or (3) for the purpose of determining a consumer's eligibility for any repayment plan; provided, however, that Customer may, consistent with the certification and limitations set forth in this Section 1, use the Non-FCRA LN Services for identifying, locating, or contacting a consumer in connection with the collection of a consumer's debt or for prioritizing collection activities; and (D) Customer shall not use any of the

information it receives through the Non-FCRA LN Services to take any “adverse action,” as that term is defined in the FCRA.

2. **General.** Customer and LNRSFL agree that: (i) capitalized terms used herein but not otherwise defined herein shall have the meanings ascribed to them in the Master Terms; (ii) this Non-FCRA Addendum modifies and amends only those specific terms of the Master Terms expressly referenced herein; and (iii) all terms of the Master Terms are hereby restated as if written herein, shall remain in full force and effect, and shall constitute the legal valid, binding and enforceable obligations of the parties; and (iv) the LexisNexis Risk Solutions Application, the Master Terms, the Non-FCRA Addendum and the Subscription Agreement are for purposes of governing the provision and use of the Non-FCRA LN Services.

AUTHORIZATION AND ACCEPTANCE OF TERMS

I HEREBY CERTIFY that I am authorized to execute this Non-FCRA Addendum on behalf of the Customer listed above.

CUSTOMER:

Signature:

Print:

Title:

Dated: (mm/dd/yy)

Accurint Virtual Crime Center/Accurint Crime Analysis/LexisNexis Community Crime Map/AVCC XML Addendum Consortium Lead-Agency (Document 10)

This Accurint Virtual Crime Center/Accurint Crime Analysis/LexisNexis Community Crime Map/AVCC XML Addendum ("Addendum") sets forth additional or amended terms and conditions for the use of Accurint Virtual Crime Center; Accurint Crime Analysis; LexisNexis Community Crime Map and/or AVCC XML (the "LN Services" provided herein), which are in addition to, and without limitation of, the terms and conditions set forth in the services agreement between the customer identified below ("Customer") and LexisNexis Risk Solutions FL Inc. or its affiliated entity ("LN") for the LN Services (such services agreement, the "Agreement"). The LN Services subscribed to herein will be listed on Customer's Schedule A. Capitalized terms used herein but not defined herein shall have the meanings ascribed to them in the Agreement.

I. Public Safety Data Exchange Database

1. LN, as a vendor that processes information for its government customers, maintains the LexisNexis Public Safety Data Exchange Database ("PSDEX"), which contains information related to public safety and law enforcement investigations. PSDEX is compiled from information submitted by PSDEX customers and enhanced by LN data and technology such as LexID or data updates to allow LN's PSDEX customers to easily search and access information beyond their jurisdiction for analysis, investigations and reporting or other applications to accomplish their mission.
2. In exchange for good and valuable consideration, including access to PSDEX, Customer hereby agrees to contribute public safety information (the "Customer Data Contribution") that it and other PSDEX customers may use for analysis, investigations and reporting or other applications to accomplish their mission.
3. LN's obligations.
    a. LN agrees to provide PSDEX information to Customer.
    b. LN agrees to provide Customer with instructions for submitting information to the PSDEX database and for using the PSDEX service.
    c. LN agrees to provide all LN employees, with physical or logical access to Customer Data Contributions, level four security awareness training as defined and listed in the Criminal Justice Information Services (CJIS) Security Policy.
    d. LN agrees to access, store, and process Customer's Customer Data Contributions in accordance with the CJIS Security Policy, to the extent applicable to LN's accessing, storage, and processing of such data.
4. Customer obligations.
    a. Customer agrees to submit to LN, with reasonable promptness and consistency, Customer Data Contributions.
    b. Customer acknowledges and agrees that it is solely responsible for the content of the Customer Data Contributions submitted to LN and that it shall use reasonable care to ensure the information submitted is a reasonable reflection of the actual report. Each submission to LN with respect to an incident or subject constitutes a Customer Data Contribution.
    c. Customer's disclosure of information to LN is and will be in compliance with all applicable laws, regulations and rulings.
    d. Customer agrees to access, store, and process other customer's Customer Data Contributions in accordance with the CJIS Security Policy, to the extent applicable to Customer's accessing, storage, and processing of such data.

e. Customer agrees to notify LN promptly of any change in status, factual background, circumstances or errors concerning any Customer Data Contribution previously provided to LN. Customer further agrees to submit corrected information in a timely manner. Customer agrees that it will fully and promptly cooperate with LN should any inquiry about the Customer Data Contributions arise.
f. The following named individual/department shall serve as the contact person(s) for submissions made to LN. The contact person shall respond to requests from LN for clarification or updates on incident reports submitted by Customer during normal business hours, and Customer will not unreasonably withhold from LN information on any such submission. LN shall not reveal the identity of the Customer's contact person(s) to any other PSDEX customer without Customer's consent.

   Name:
   Title:
   Address:
   Phone:
   Fax:
   Email:

g. Customer agrees that it will access information contributed to PSDEX by other customers only through LN and any Customer employee permitted access to PSDEX by Customer shall be a CJI Authorized User/Personnel that has undergone appropriate Security Awareness Training as those terms are used in the CJIS Security Policy.
h. Customer agrees that, to the extent permitted under applicable law, LN and all other PSDEX customers shall not be liable to Customer, and Customer hereby releases LN and all other PSDEX customers from liability to Customer, for any claims, damages, liabilities, losses and injuries arising out of, or caused in whole or in part by LN or each such other PSDEX customer's acts and omissions in reporting or updating Customer Data Contributions for inclusion in PSDEX. Other PSDEX customers are intended to be third party beneficiaries of this paragraph.

II. General Terms

1. **LICENSE GRANT**. Customer, at no charge, hereby grants to LN a paid up, irrevocable, worldwide, non-exclusive license to use, adapt, compile, aggregate, create derivative works, transfer, transmit, publish and distribute the Customer Data Contributions (1) to PSDEX customers; and (2) by agreement by initialing below, a de-identified subset (e.g., crime type, date/time of the incident, and the area that the incident has occurred) to third-parties assisting the public with a view of de-identified crime data. For purposes of clarification, Customer is the owner of its Customer Data Contributions and is hereby licensing to LN a copy of its Customer Data Contributions.

   Customer will not provide a de-identified subset of its data to third parties (initials).

2. **FBI CJIS SECURITY ADDENDUM**. This Addendum incorporates by reference the requirements of the FBI CJIS Security Policy and the FBI CJIS Security Addendum (FBI CJIS Security Policy Appendix H attached hereto as Exhibit A), as in force as of the date of this Addendum and as may, from time to time hereafter, be amended. The parties warrant that they have the technological capability to handle Criminal Justice Information (CJI), as that term is

defined by the FBI CJIS Security Policy, in the manner required by the CJIS Security Policy. The parties expressly acknowledge that the CJIS Security Policy places restrictions and limitations on the access to, use of, and dissemination of CJI and hereby warrant that their respective systems abide by those restrictions and limitations.

3. **GOOGLE GEOCODER**. LN uses Google Geocoder to geocode address locations that do not already contain "X" and "Y" coordinates. Any "X" and "Y" coordinate information provided by the Customer is assumed by LN to be accurate and will not be geocoded by Google Geocoder. Crime dot locations geocoded by Google Geocoder as displayed in PSDEX are approximate due to automated location methods and address inconsistencies.
4. **DATA DISCLAIMER**. LN is not responsible for the loss of any data or the accuracy of the data, or for any errors or omissions in the LN Services or the use of the LN Services or data therein by any third party, including the public or any law enforcement or governmental agencies. Due to the nature of the origin of public safety information, the data contained in PSDEX may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. The LN Services aggregate and report data as provided by PSDEX customers and is not the source of the data, nor is it a comprehensive compilation of all law enforcement data. Before Customer relies on any data, it should be independently verified.
5. **LINKS TO THIRD PARTY SITES.** PSDEX may contain links or produce search results that reference links to third party websites ("Linked Sites"). LN has no control over these Linked Sites or the content within them. LN cannot and does not guarantee, represent, or warrant that the content contained in the Linked Sites, including, without limitation other links, is accurate, legal, and/or inoffensive. LN does not endorse the content of any Linked Site, nor does it warrant that a Linked Site will not contain computer viruses or other harmful code. By using PSDEX to search for or link to Linked Sites, Customer agrees and understands that such use is entirely at its own risk, and that Customer may not make any claim against LN for any damages or losses whatsoever resulting from such use.
6. **OWNERSHIP OF SUBMITTED CONTENT**. All information provided by a PSDEX customer is offered and owned by that customer. Unless otherwise indicated by written request from Customer, all data will be retained by LN and remain accessible by others in accordance with the provisions of this Addendum.

AUTHORIZATION AND ACCEPTANCE

I HEREBY CERTIFY that I am authorized to execute this Addendum on behalf of Customer.

Required: Customer ORI number (Originating Agency Identifier):

CUSTOMER:
Signature:
Print:
Title:
Date:

Exhibit A

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.
1.00 Definitions
1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.
1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.
2.00 Responsibilities of the Contracting Government Agency.
2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).
3.00 Responsibilities of the Contractor.
3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).
4.00 Security Violations.
4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.
4.02 Security violations can justify termination of the appended agreement.
4.03 Upon notification, the FBI reserves the right to:
a. Investigate or decline to investigate any report of unauthorized use;
b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after

satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

Accurint Virtual Crime Center/Accurint Crime Analysis/LexisNexis Community Crime Map/AVCC XML Addendum Consortium Sub-Agency (Document 11)

This Accurint Virtual Crime Center/Accurint Crime Analysis/LexisNexis Community Crime Map/AVCC XML Addendum ("Addendum") sets forth additional or amended terms and conditions for the use of Accurint Virtual Crime Center; Accurint Crime Analysis; LexisNexis Community Crime Map; and/or AVCC XML (the "LN Services" provided herein), which are in addition to, and without limitation of, the terms and conditions set forth in the services agreement between the Consortium Lead Agency and LexisNexis Risk Solutions FL Inc. or its affiliated entity ("LN") for the LN Services (such services agreement, the "Agreement"). As the Consortium Sub-Agency signing below ("Customer"), your use of the LN Services is subject to the Agreement signed by the Consortium Lead Agency identified above, and this Addendum. A substantially similar version of the Agreement may be found at http://www.lexisnexis.com/risk/masterterms/government/. The LN Services subscribed to herein will be .
Capitalized terms used herein but not defined herein shall have the meanings ascribed to them in the Agreement.

I. Public Safety Data Exchange Database

1. LN, as a vendor that processes information for its government customers, maintains the LexisNexis Public Safety Data Exchange Database ("PSDEX"), which contains information related to public safety and law enforcement investigations. PSDEX is compiled from information submitted by PSDEX customers and enhanced by LN data and technology such as LexID or data updates to allow LN's PSDEX customers to easily search and access information beyond their jurisdiction for analysis, investigations and reporting or other applications to accomplish their mission.
2. In exchange for good and valuable consideration, including access to PSDEX, Customer hereby agrees to contribute public safety information (the "Customer Data Contribution") that it and other PSDEX customers may use for analysis, investigations and reporting or other applications to accomplish their mission.
3. LN's obligations.
    a. LN agrees to provide PSDEX information to Customer.
    b. LN agrees to provide Customer with instructions for submitting information to the PSDEX database and for using the PSDEX service.
    c. LN agrees to provide all LN employees, with physical or logical access to Customer Data Contributions, level four security awareness training as defined and listed in the Criminal Justice Information Services (CJIS) Security Policy.
    d. LN agrees to access, store, and process Customer's Customer Data Contributions in accordance with the CJIS Security Policy, to the extent applicable to LN's accessing, storage, and processing of such data.
4. Customer obligations.
    a. Customer agrees to submit to LN, with reasonable promptness and consistency, Customer Data Contributions.
    b. Customer acknowledges and agrees that it is solely responsible for the content of the Customer Data Contributions submitted to LN and that it shall use reasonable care to ensure the information submitted is a reasonable reflection of the actual report. Each submission to LN with respect to an incident or subject constitutes a Customer Data Contribution.

d. Customer agrees to access, store, and process other customer's Customer Data Contributions in accordance with the CJIS Security Policy, to the extent applicable to Customer's accessing, storage, and processing of such data.
e. Customer agrees to notify LN promptly of any change in status, factual background, circumstances or errors concerning any Customer Data Contribution previously provided to LN. Customer further agrees to submit corrected information in a timely manner. Customer agrees that it will fully and promptly cooperate with LN should any inquiry about the Customer Data Contributions arise.
f. The following named individual/department shall serve as the contact person(s) for submissions made to LN. The contact person shall respond to requests from LN for clarification or updates on incident reports submitted by Customer during normal business hours, and Customer will not unreasonably withhold from LN information on any such submission. LN shall not reveal the identity of the Customer's contact person(s) to any other PSDEX customer without Customer's consent.

   Name:
   Title:
   Address:
   Phone:
   Fax:
   Email:

g. Customer agrees that it will access information contributed to PSDEX by other customers only through LN and any Customer employee permitted access to PSDEX by Customer shall be a CJI Authorized User/Personnel that has undergone appropriate Security Awareness Training as those terms are used in the CJIS Security Policy.
h. Customer agrees that, to the extent permitted under applicable law, LN and all other PSDEX customers shall not be liable to Customer, and Customer hereby releases LN and all other PSDEX customers from liability to Customer, for any claims, damages, liabilities, losses and injuries arising out of, or caused in whole or in part by LN or each such other PSDEX customer's acts and omissions in reporting or updating Customer Data Contributions for inclusion in PSDEX. Other PSDEX customers are intended to be third party beneficiaries of this paragraph.

II. General Terms

1. **LICENSE GRANT**. Customer, at no charge, hereby grants to LN a paid up, irrevocable, worldwide, non-exclusive license to use, adapt, compile, aggregate, create derivative works, transfer, transmit, publish and distribute the Customer Data Contributions (1) to PSDEX customers; and (2) by agreement by initialing below, a de-identified subset (e.g., crime type, date/time of the incident, and the area that the incident has occurred) to third-parties assisting the public with a view of de-identified crime data. For purposes of clarification, Customer is the owner of its Customer Data Contributions and is hereby licensing to LN a copy of its Customer Data Contributions.

   Customer will not provide a de-identified subset of its data to third parties (initials).

2. **FBI CJIS SECURITY ADDENDUM**. This Addendum incorporates by reference the requirements of the FBI CJIS Security Policy and the FBI CJIS Security Addendum (FBI CJIS

Security Policy Appendix H attached hereto as Exhibit A), as in force as of the date of this Addendum and as may, from time to time hereafter, be amended. The parties warrant that they have the technological capability to handle Criminal Justice Information (CJI), as that term is defined by the FBI CJIS Security Policy, in the manner required by the CJIS Security Policy. The parties expressly acknowledge that the CJIS Security Policy places restrictions and limitations on the access to, use of, and dissemination of CJI and hereby warrant that their respective systems abide by those restrictions and limitations.

3. **GOOGLE GEOCODER**. LN uses Google Geocoder to geocode address locations that do not already contain "X" and "Y" coordinates. Any "X" and "Y" coordinate information provided by the Customer is assumed by LN to be accurate and will not be geocoded by Google Geocoder. Crime dot locations geocoded by Google Geocoder as displayed in PSDEX are approximate due to automated location methods and address inconsistencies.
4. **DATA DISCLAIMER**. LN is not responsible for the loss of any data or the accuracy of the data, or for any errors or omissions in the LN Services or the use of the LN Services or data therein by any third party, including the public or any law enforcement or governmental agencies. Due to the nature of the origin of public safety information, the data contained in PSDEX may contain errors. Source data is sometimes reported or entered inaccurately, processed poorly or incorrectly, and is generally not free from defect. The LN Services aggregate and report data as provided by PSDEX customers and is not the source of the data, nor is it a comprehensive compilation of all law enforcement data. Before Customer relies on any data, it should be independently verified.
5. **LINKS TO THIRD PARTY SITES.** PSDEX may contain links or produce search results that reference links to third party websites ("Linked Sites"). LN has no control over these Linked Sites or the content within them. LN cannot and does not guarantee, represent, or warrant that the content contained in the Linked Sites, including, without limitation other links, is accurate, legal, and/or inoffensive. LN does not endorse the content of any Linked Site, nor does it warrant that a Linked Site will not contain computer viruses or other harmful code. By using PSDEX to search for or link to Linked Sites, Customer agrees and understands that such use is entirely at its own risk, and that Customer may not make any claim against LN for any damages or losses whatsoever resulting from such use.
6. **OWNERSHIP OF SUBMITTED CONTENT**. All information provided by a PSDEX customer is offered and owned by that customer. Unless otherwise indicated by written request from Customer, all data will be retained by LN and remain accessible by others in accordance with the provisions of this Addendum.

AUTHORIZATION AND ACCEPTANCE

I HEREBY CERTIFY that I am authorized to execute this Addendum on behalf of Customer.

Required: Customer ORI number (Originating Agency Identifier):

CUSTOMER:
Signature:
Print:
Title:
Date:

Exhibit A

FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.
1.00 Definitions
1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.
1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.
2.00 Responsibilities of the Contracting Government Agency.
2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).
3.00 Responsibilities of the Contractor.
3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).
4.00 Security Violations.
4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.
4.02 Security violations can justify termination of the appended agreement.
4.03 Upon notification, the FBI reserves the right to:
a. Investigate or decline to investigate any report of unauthorized use;
b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after

satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306