NATIONAL INSURANCE CRIME BUREAU

LAW ENFORCEMENT ISO CLAIMSEARCH ACCESS MEMORANDUM OF UNDERSTANDING

This Law Enforcement ISO ClaimSearch Access Memorandum of Understanding ("MOU") is made and entered into by and between the National Insurance Crime Bureau ("NICB"), an Illinois not-for-profit corporation located at 1111 E. Touhy Avenue, Suite 400, Des Plaines, Illinois 60018 and the law enforcement agency identified on the signature page hereto ("Agency") ("NICB" and, together with "Agency," hereafter referred to from time to time individually as "Party" or collectively as "the Parties") and is effective as of the date of the last signature to this Agreement ("Effective Date").

RECITALS

WHEREAS, NICB is an Illinois not-for-profit corporation dedicated to fighting insurance-related crime and fraud, and gathering and disseminating information related to insurance crime and fraud for the benefit of NICB member companies, law enforcement, regulatory authorities and the general public; and

WHEREAS, Verisk Analytics Inc. ("Verisk") owns ISO ClaimSearch, and NICB contracts with Verisk in order to credential and provide law enforcement agencies and their personnel access to ISO ClaimSearch on the condition that NICB pass through certain terms to the law enforcement agency;

WHEREAS, Agency is a law enforcement agency whose mission is to protect and serve the people of the applicable jurisdiction; and

WHEREAS, NICB and Agency desire to work together to exchange information and data that will allow both Parties to more easily detect and prevent insurance-related crime and fraud;

NOW THEREFORE, in consideration of the promises and obligations contained in this MOU, and other good and valuable consideration the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Access. Subject to the terms of this MOU, during the Term, NICB hereby grants to Agency a non-exclusive, non-transferable, non-assignable, limited, revocable right to allow employees with access credentials within their organization the right to access and use the ISO ClaimSearch for: (1) investigating or prosecuting crime, including but not limited to insurance-related crime and fraud; and (2) investigating or prosecuting individuals relevant to homeland security activity. (collectively the "Purpose").

2. Access Credentials. In order to access the ISO ClaimSearch, Agency must appoint an administrator ("Administrator") to receive access credentials to the ISO ClaimSearch. The Administrator, in turn, may designate individuals employed by Agency ("Designees") to receive access credentials to ISO ClaimSearch.

3. Confidentiality.

    A. All non-public information and data contained within ISO ClaimSearch pursuant to this Agreement shall be considered as confidential information

("Confidential Information"). Confidential Informational shall be held in the strictest confidence and shall not be released, disseminated, used, accessed, copied, shared, transferred, or disclosed by Agency, except as strictly necessary for the Purpose.

B. Confidential Information shall not include any information, however designated or marked, that: (i) is publicly available, or subsequently becomes publicly available, after the time it was communicated to the recipient through no breach of this MOU by the recipient; (ii) was in the recipient's possession free of any obligation of confidence prior to being communicated to the recipient by the disclosing party, or is in the recipient's possession free of any obligation of confidence subsequent to the time it was communicated to the recipient by the disclosing party; (iii) is independently developed by employees or agents, without use of the data contained in the ISO ClaimSearch, of the recipient and can be so proven by recipient; or (iv) is obtained by the receiving party from a third party lawfully in possession of such information and without a breach of such third party's obligations of confidentiality.

C. It shall not be a violation of Section 3 of this MOU for Agency to disclose Confidential Information as required by standard legal procedure in order to prosecute crime. Further, disclosure is permitted in response to a lawful subpoena or other legal process served upon Agency or where applicable law requires the disclosure of Confidential Information, provided that: (i) if not prohibited under applicable law, Agency, prior to disclosing such information, gives reasonable written notice to NICB sufficient to permit NICB to seek a protective order if it so chooses; and (ii) in all cases, Agency discloses only that information that is legally required to be disclosed. For clarity, any of the Confidential Information Agency discloses pursuant to this Section 3. c. shall remain subject to the confidentiality requirements under this MOU for all other purposes.

4. Agency Obligations. In exchange for access to ISO ClaimSearch, the Agency agrees to comply with the following obligations:

A. Administrator. Agency shall appoint an Administrator who shall be identified to NICB and shall be responsible for adding or removing Designees, as appropriate, as well as maintaining a list of active Designees. No Designee may be granted access to ISO ClaimSearch without Administrator approval. The Administrator shall be the Agency contact responsible for fulfilling Agency obligations required under this MOU.

B. Designees. Designees shall be restricted to active Agency employees who: (1) are in good standing and not under suspension for any criminal or civil violation, or under active criminal investigation or indictment ("Good Standing"); and (2) have a need to know the Confidential Information for the Purpose.

C. Vetting. Agency shall have in place a vetting process to ensure minimum standards for each Designee to qualify for access to ISO ClaimSearch are met, including the following determinations for each Designee:

   i. the Designee's need for access;

   ii. which level of access is required for the Designee and for what purpose;

   iii. ensuring Designee's access conforms to this Agreement;

   iv. ensuring Designee's access is based on the Designee's need to know in order to carry out the Purpose; and

   v. documenting the above determinations.

D. Responsibility. The Administrator shall be responsible for, and shall supervise and control, all Designee access to ISO ClaimSearch. The Administrator shall implement an internal process whereby Designee usage is documented and monitored to ensure that that Designee usage conforms with the Purpose and this MOU. Agency shall immediately notify NICB of any access or usage of ISO ClaimSearch that does not comply with this Agreement and shall prohibit Designee from any further access or usage of ISO ClaimSearch until future access is expressly approved, in writing, by NICB.

E. Training. Agency shall ensure that Designees complete all training and certifications required in order to gain access; and all periodic training either assigned by NICB, the ISO ClaimSearch platform, or otherwise in order to maintain access.

F. Termination of Access. Agency shall immediately terminate Designee's access to ISO ClaimSearch:

   i. when Designee's is no longer employed by Agency;

   ii. when Designee no longer has a legitimate Purpose to have access to ISO ClaimSearch; or

   iii. if a Designee is no longer in Good Standing.

G. Privacy and Security Policies. Agency will, at all times, ensure that access and use of ISO ClaimSearch complies with the NICB Privacy and Security Policy, and the ISO Privacy and Security Policies, including any updates and amendments that may be issued from time to time.

H. Controls for the Protection of Confidential Information. Agency shall maintain during the term of this MOU, and at all times thereafter in which Agency maintains Confidential Information in its possession or control, an information security program that provides for the administrative, technical, and physical safeguards designed to adequately protect the security and confidentiality of Confidential Information in Agency's possession or control in accordance with

applicable federal, state and local laws, rules, and regulations. At a minimum, Agency's safeguards for the protection of Confidential Information shall include:

i. limiting access of Confidential Information to authorized employees;

ii. maintaining an adequate network firewall;

iii. securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including but not limited to devices with information storage capability;

iv. implementing secure storage and disposal of Confidential Information;

v. implementing authentication, and access controls within operating systems and equipment; and

vi. implementing appropriate personnel security and integrity procedures and practices, including conducting background checks consistent with applicable law and providing appropriate privacy and information security training to Agency employees.

5. Audits. NICB may issue a security assessment questionnaire and conduct independent onsite security assessments of Agency related to Agency's compliance this Agreement. For any onsite inspection, NICB will provide at least 30 days prior written notice. Such assessments shall not occur more than once per calendar year, at a time that minimizes operational interruptions to Agency. Agency's failure to adequately respond in a timely manner to a security assessment questionnaire, timely submit to an onsite inspection, or timely or adequately, in NICB's sole determination, remedy any compliance or security concern raised by NICB, may result in immediate suspension of Agency's ISO ClaimSearch access pursuant to Section 10 of the MOU.

6. Security Breach.

A. Notification. Agency shall promptly, but in no case later than 48 hours, notify NICB of any confirmed or based on a good faith determination by NICB or Agency there is a significant risk to Confidential Information unauthorized or improper access to or use or disclosure of Confidential Information while in the possession or control of Agency, its Administrator or its Designees ("Security Breach").

B. Mitigation and Cooperation. Agency shall promptly implement steps to remediate and mitigate the effects of any Security Breach. Agency shall cooperate with reasonable requests for information from NICB or its representatives regarding the Security Breach. To the extent possible, Agency shall promptly provide a written description of the number of individuals' data involved, the location (i.e., State) of the individuals, the amount of data involved, the type of data involved and any other relevant information

reasonably requested by NICB or as otherwise required to be provided by applicable law.

7. Representations and Warranties. Agency represents and warrants the following:

   A. Agency is a professional, reputable, and trustworthy organization that serves the public.

   B. Agency is not under suspension for any criminal or civil violation; or under active criminal investigation or indictment.

   C. Agency will not provide access to any Designee who is not in Good Standing.

   D. Agency, its Administrator, and its Designees have a justifiable reason for requiring access to ISO ClaimSearch that is consistent with the Purpose.

   E. Agency either (a) has an established working relationship with NICB, or (b) will take steps in order to establish a new relationship with NICB.

   F. Agency agrees to comply with all applicable federal, state, and local data privacy and security laws, rules and regulations, and applicable industry standards related to or concerning the protection of data.

8. Indemnity. To the extent permissible by law, Agency shall indemnify, defend and hold NICB harmless from all third-party lawsuits, claims, liabilities, damages, settlements, judgments, or expenses, including NICB's costs and reasonable attorney fees, which arise as a result of Agency's material breach of this Agreement, negligent acts or omissions, or willful misconduct.

9. Disclaimer of Warranties. Limited Use; No Reliance. Information contained within ISO ClaimSearch is provided "AS IS, WHERE IS" and intended to be used as investigative leads only, in support of investigations of criminal activity in accordance with the Purpose. Agency should not make prosecution decisions based solely upon information contained in ISO ClaimSearch. NICB HEREBY DISCLAIMS ALL WARRANTIES EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE INFORMATION CONTAINED WITHIN ISO CLAIMSEARCH.

10. Term and Termination.

   A. Term. This MOU shall commence as of the Effective Date and will remain in effect until either Party terminates this MOU by providing 30 days' written notice to the other party of the termination whereupon the MOU will terminate at the end of the 90-day notice period.

   B. Immediate Termination. NICB may immediately terminate this MOU if the Agency materially breaches its obligations under this MOU.

11. Survival. Upon termination of this MOU, the provisions of this MOU concerning the ongoing interests of the parties shall continue and survive in full force and effect.

12. Assignment. Neither Party may assign or transfer any rights or obligations under this MOU without the prior written consent of the other Party. Any attempt to transfer all or part of either Party's rights or obligations without such consent is null and void and of no effect.

13. Notices. All notices between the parties will be in writing and will be delivered as follows, with notice deemed given as indicated (a) by personal delivery, when delivered personally; or (b) by overnight courier, upon the courier's confirmation of delivery. In either case, a copy shall be sent via email. Notices to the Agency will be sent to the email and address provided by Agency at the time of application for credentialing. Notices to NICB will be sent to the addresses, including e-mail addresses, set forth as follows, or such other address as is provided by notice as set forth herein:

    National Insurance Crime Bureau
    1111 E. Touhy Avenue, Suite 400
    Des Plaines, Illinois 60018
    Attn: General Counsel
    Email: pmartin@nicb.org; rcooper@nicb.org

14. Severability. Any term or provision of this MOU held to be illegal or unenforceable will, if possible, be interpreted so as to be construed as valid, but in any event the validity or enforceability of the remainder hereof will not be affected.

15. No Waiver. The waiver of, or failure to enforce, any breach or default hereunder will not constitute the waiver of any other or subsequent breach or default.

16. No Joint Venture. The relationship of the parties hereunder will be that of two independent contracting parties, and nothing herein will be deemed to create a joint venture, partnership, agency or employer/employee relationship. In no event will either party be permitted to make any MOU, or represent that it is authorized to make any MOU, on behalf of the other party, without the prior written consent of such other party.

17. Entire Agreement. This MOU sets forth the entire agreement between the parties related to the subject matter herein, and supersedes any and all prior agreements, proposals, understandings, discussions, MOUs, and representations between them, whether written or oral. This MOU may be changed only by mutual MOU of the parties in writing. This MOU may be executed in counter-parts with electronic signatures to be deemed valid and binding.

[*Signatures immediately to follow on page 7 of 7*]

IN WITNESS WHEREOF, the parties hereto have caused this MOU to be executed by their duly authorized representatives.

National Insurance Crime Bureau	Agency: _____
	ORI: _____
Signed: _____	Signed: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____