SEVENTH AMENDATORY AGREEMENT

This **SEVENTH AMENDATORY AGREEMENT** is made and entered into by and between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the "City"), and **LEXISNEXIS CLAIMS SOLUTIONS INC.**, a whose address is 1000 Alderman Drive, Alpharetta, Georgia 30005 (the "Vendor") collectively, the "Parties".

WITNESSETH:

WHEREAS, the Parties entered into an Agreement dated November 29, 2011 and amended the Agreement on October 25, 2012, January 27, 2014, July 13, 2015, February 15, 2017, and July 24, 2017, (the "Agreement"), to replace the Denver Police Department's homegrown Offense reporting System with the preferred solution of the enterprise Record Management System (Versaterm) within the Denver Police Department where the public can order and pay for police reports and;

WHEREAS, the Parties acknowledge and agree that LexisNexis Claims Solutions Inc. is the successor in interest to Coplogic Inc., and

WHEREAS, the Parties wish to amend the terms of the Agreement, including an extension of the term and increase compensation to the Vendor;

WHEREAS, the Parties acknowledge and agree that Sixth Amendatory Agreement was inadvertently skipped and the last amendment to the Agreement was the Fifth Amendatory Agreement,

NOW, THEREFORE, in consideration of the premises and the mutual covenants and obligations herein set forth, the Parties agree as follows:

1. Article 2 of the Agreement entitled "GRANT OF LICENSE; RESTRICTIONS" is hereby modified to delete subsection (A) and replace with the following:

2.

"A. Vendor hereby grants to City a restricted, limited, revocable license to use the Software only as set forth in this Agreement, and for no other purposes, subject to the restrictions and limitations set forth below:

a. City shall not use the Software for marketing or commercial solicitation purposes, resell, or broker the Software to any third-party or otherwise use the Software for any personal (non-law enforcement) purposes; and

b. City shall not access or use Software from outside the United States without Vendor's prior written approval; and

c. City shall not use the Software to create a competing product or provide data processing services to third parties; and

d. City's use of the Software hereunder will not knowingly violate any agreements to which City is bound; and

e. City shall not harvest, post, transmit, copy, modify, create derivative works from, tamper, distribute the Software, or in any way circumvent the navigational structure of the Software, including to upload or transmit any computer viruses, Trojan Horses, worms or anything else designed to interfere with, interrupt or disrupt the normal operating procedures of Software; and

f. City may not 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 or otherwise infringe on the rights of others; and

g. City shall not reveal any user accounts or passwords for the Software to any third parties (third parties shall not include City's employees who have a need to know such information); and

h. City shall not permit any third party (third parties shall not include City's employees who have a need to know such information) to view or use the Software (even if such third party is under contract to provide services to City); notwithstanding the foregoing, City may permit contractors to have access to view the Software if the contractor has a need to access the Software to perform their hired function and is bound in writing to maintain the confidentiality of, and not to use, Vendor's Confidential Information under terms and conditions no less stringent than those set forth in this Agreement; and

i. City shall comply with all laws, regulations, and rules which govern the use of the Software."

3. Article 4 of the Agreement entitled "**TERM**" is hereby amended to read as follows:

"**4**. **TERM**: The term of the Agreement is from October 1, 2011 through December 31, 2022."

4. Articles 5.A. and 5.D(i) of the Agreement entitled "**Fee**" and "**Maximum Contract Liability**" are hereby amended to read as follows:

"**5**. **COMPENSATION AND PAYMENT**:

A. Fee: The fee for the software and services described in Exhibits A and A-1 is **SEVEN HUNDRED SIXTY-FOUR THOUSAND FIVE HUNDRED NINETY-SEVEN DOLLARS ($764,597.00)** (the "Fee"). The Fee shall be paid pursuant to the City's Prompt Payment Ordinance.

D. Maximum Contract Liability:

(i) Any other provision of this Agreement notwithstanding, in no event shall the City be liable for payment for services rendered and expenses incurred by Vendor under the terms of this Agreement for any amount in excess of the sum of **SEVEN HUNDRED S I X T Y -FOUR THOUSAND FIVE HUNDRED NINETY-SEVEN DOLLARS ($764,597.00)**. Vendor acknowledges that any work performed by Vendor beyond that specifically authorized by the City is performed at Vendor's risk and without authorization under this Agreement. City acknowledges that Vendor shall not be required to travel on-site to perform work."

5. Exhibit B, "Security", shall be deleted in its entirety and replaced with the following:

"A. Vendor Security Requirements:

(i). Vendor shall have in place documented policies and procedures, which shall be reviewed, and if appropriate, tested and updated, as appropriate, covering the administrative, physical and technical safeguards in place and relevant to the access, use, loss, alteration, disclosure, storage, destruction and control of information and which are measured against objective standards and controls. Such program shall comply with all applicable laws.

(ii). Vendor's Information Security Program shall:
a) account for known and reasonably anticipated risks and threats, and Vendor shall, on an ongoing basis, monitor for new threats;
b) meet or exceed industry best practices;
c) ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
d). Address physical security inclusive of ensuring that physical access to facilities is restricted and controlled to allow access only to authorized personnel, and that such physical access is terminated when no longer needed;
e). Require that any individual or entity acting under the authority of Vendor and who has access to personal data does not process such data except as required to do so by City, unless required to do so by applicable law, and that such individuals or entities are committed to maintaining confidentiality of such personal data as required by law;
f). Access control and management including the identification, authentication and control of access to, and use of, information, facilities, networks, computers and software including deactivation of credentials when no longer needed.

(iii). Vendor Security Event.

As used herein, "City Data" shall mean data or information that is owned or controlled by City and that is provided to Vendor and to which Vendor has access to and it otherwise processes for the provision of the Software or services under the Agreement, and that uniquely identifies a natural person, including: (i) first and last name or first initial and last name; (ii) a home or other physical address, which includes at least a street name and name of city or town; (iii) an email address; (iv) a telephone number; when the foregoing are included in combination with either a: (i) a social security number; (ii) credit and/or debit card information, including credit and/or debit card number with expiration date; ((iii) driver's license number. City Data shall not include (i) incidents in which, after an appropriate investigation, Vendor reasonably determines that a breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed; (ii) any unintentional acquisition, access, or use of City Data by a Vendor employee or person acting under the authority of Vendor, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the Agreement; (iii) any inadvertent disclosure by a person who is authorized to access City Data; (iv) a disclosure of City Data where Vendor has a good faith belief that an unauthorized person to whom the disclosure was made did not reasonably reuse or re-disclose such City Data.

In the event Vendor confirms that City Data has been disclosed to an unauthorized party (a "Vendor Security Event") Vendor shall, if required by applicable law, and without disclosing information that is protected by the attorney-client privilege or otherwise confidential:
(i) promptly notify City and investigate the situation; and
(ii) upon request, provide a reasonable summary of the circumstances surrounding such Vendor Security Event to City; and
(iii) cooperate reasonably with City's requests for information regarding such Vendor Security Event;
(iv) notify the impacted individuals and any other third parties as may be required by law.
(v) bear all costs associated with complying with its legal and regulatory obligations in connection therewith; and
(vi) be responsible for the legal obligations and any associated costs which may arise under applicable law in connection with such a Vendor Security Event, including, but not limited to: litigation (including attorney's fees); reimbursement sought by individuals (including costs for credit monitoring and other losses alleged to be in connection with such Vendor Security Event).

B. City Security Requirements:

(i). Data Protection.
City shall take appropriate measures to protect against the misuse and unauthorized access through or to City's (i) credentials ("Account IDs") used to access the Software; or (ii) corresponding passwords, whether by City or any third party. City shall manage identification, use, and access control to all Account IDs in an appropriately secure manner and shall promptly deactivate any Account IDs when no longer needed or where access presents a security risk. City shall implement its own appropriate program for Account ID management and shall use commercially reasonable efforts to follow the policies and procedures for account maintenance as determined by industry best practices.

(ii). City's Information Security Program.
City shall implement and document, or follow its existing, appropriate policies and procedures covering the administrative, physical and technical safeguards in place and relevant to the access, use, storage, destruction, and control of information which are measured against objective standards and controls ("City's Information Security Program"). City's Information Security Program shall: (1) account for known and reasonably anticipated threats and City shall monitor for new threats on an ongoing basis; and (2) meet or exceed industry best practices as determined by City to be commercially practicable. City will promptly remediate any deficiencies identified in City's Information Security Program. City shall not allow the transfer of any personally identifiable information received from Vendor across any national borders outside the United States without the prior written consent of Vendor.

(iii). City Security Event.
In the event City learns or has reason to believe that Account IDs have been misused, disclosed, or accessed in an unauthorized manner or by an unauthorized person, solely as a result of the City's acts or omissions, (a "City Security Event") City shall:
(i) provide immediate written notice to:
a) the Information Security and Compliance Organization at 1000 Alderman Drive,

Alpharetta, Georgia 30005; or
b) via email to (security.investigations@lexisnexis.com); or
c) by phone at (1-888-872-5375) with a written notification to follow within twenty four (24) hours; and
(ii) promptly investigate the situation; and
(iii) obtain written consent from Vendor, not to be unreasonably withheld, prior to disclosing Vendor or the Software to any third party in connection with the City Security Event; and
(iv) if required by law and agreeing to give due consideration to regulatory guidance, including any such guidance relating to impact to data subjects, City shall:
a) notify the individuals whose information was disclosed that a City Security Event has occurred; and
b) be responsible for all legal and regulatory obligations including any associated costs which may arise in connection with the City Security Event; and
(v) remain solely liable for all costs and claims that may arise from the City Security Event, including, but not limited to: litigation (including attorney's fees); reimbursement sought by individuals (including costs for credit monitoring and other losses alleged to be in connection with such City Security Event); and
(vi) provide all proposed third party notification materials to Vendor for review and approval prior to distribution.

In the event of a City Security Event, Vendor may, in its sole discretion, take immediate action, including suspension or termination of City's account, without further obligation or liability of any kind.

6. Exhibit B, System Availability and Performance shall be deleted in its entirety and replaced with the following:

"The Application Service Vendor will meet all system uptime, system delivery, and reliability requirements as agreed to by the Parties."

7. A new Section 41 shall be added, titled "Relevant Laws" and shall read as follows:

"41. Relevant Laws.

Each Party shall comply with all applicable federal, state, and local laws and regulations in the performance of or pursuant to the obligations under this Agreement, including:

Driver's Privacy Protection Act. City acknowledges that certain Software provided under this Agreement may include the provision of certain personal information from a motor vehicle record obtained by Vendor from state Departments of Motor Vehicles as those terms are defined by the Federal Driver's Privacy Protection Act, 18 U.S.C. § 2721 et seq., ("DPPA") and its state analogues ("DMV Data"), and that City is required to comply with the DPPA or its state analogues, as applicable. City agrees that it may be required to certify its permissible use of DPPA or DMV Data at the time it requests information in connection with certain Software and will recertify upon request by Vendor.

Fair Credit Reporting Act. The Software provided pursuant to this Agreement 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. City certifies that it will not use any of the information it receives through the Software in whole or in part as a factor in determining eligibility for credit, insurance, or employment or for any other eligibility purpose that would qualify the information in as a consumer report

Protected Health Information. Unless otherwise contemplated by an applicable Business Associate Agreement executed by the Parties, City will not provide Vendor 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.

Social Security Numbers. Social Security Numbers may be available hereunder as part of Reports and/or related data provided from certain states. However, City shall not provide Social Security Numbers to Vendor under any circumstance under this Agreement. Should City require more information on Social Security Numbers or its obligations in relation thereto, City should contact Vendor City Service at 1-866-215-2771 for assistance.

Privacy Principles. City shall comply with the "Vendor Data Privacy Principles" available at http://www.lexisnexis.com/privacy/data-privacy-principles.aspx, as updated from time to time. Vendor shall notify City in writing in the event that material changes are made to the Vendor Data Privacy Principles."

8. Except as herein amended, the Agreement is affirmed and ratified in each and every particular.

[SIGNATURE PAGES FOLLOW]

Contract Control Number:

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at Denver, Colorado as of

SEAL

CITY AND COUNTY OF DENVER

ATTEST:

By_____

_____

APPROVED AS TO FORM:

REGISTERED AND COUNTERSIGNED:

By_____

By_____

By_____

Contract Control Number: TECHS-201101011-07

Contractor Name: LEXISNEXIS CLAIMS SOLUTIONS INC.

By: _____

Name: William S. Madison
(please print)

Title: Executive Vice President
(please print)

ATTEST: [if required]

By: _____

Name: Lorraine M. Noll
(please print)

LORRAINE M NOLL
NOTARY PUBLIC
Fulton County
State of Georgia
My Comm. Expires Jan. 10, 2020

Title: _____
(please print)