Caliber Public Safety Accurint Embedded Query Credentialing Program

OVERVIEW

Colossus, Incorporated (herein referred to as "Caliber Public Safety", "Caliber", or "CPS") has partnered with LexisNexis (herein referred to as "LN") to offer for resale access to Accurint Public Data Queries embedded within Caliber Public Safety products. The LN Accurint reseller agreement requires Caliber to implement a credentialing process that investigates and confirms the identity of Organizations subscribing to the embedded Accurint Public Data Query service that will be offered via Caliber Public Safety Software products. The credentialing process will utilize credible third-party resources to confirm information submitted in the Caliber Public Safety Embedded Accurint Query Application.

CREDENTIALING OBLIGATIONS FOR END USER VERIFICATION AND INVESTIGATION

Caliber Public Safety has reviewed Appendix V of the LN Non-FCRA Government Reseller Agreement and will abide by the business practices that are stated. Caliber will perform the below activities in compliance with the Credentialing program:

1. Each Applicant requesting access to the Caliber embedded Accurint Public Data Query service shall complete an Application process, Permissible Purposes Certification, and execute an End User License Agreement (EULA) to confirm the following information. See Caliber Public Safety Embedded Accurint Query Application (herein referred to as "Application").
    a. Applicant holds a valid maintenance or subscription agreement with Caliber for access to Caliber products.
    b. Applicant is a known entity with law enforcement responsibilities (local law enforcement agencies) located within the United States.
    c. Verification of Applicant's website to verify legitimacy. If Applicant does not have a website, documentation from Applicant in the form of an email or fax confirming the lack of a website.
    d. If receiving Applicant information via fax, verify the fax header matches Applicant's entity name and physical location. If fax header does not match, collect two (2) additional business documents that verify the name and address of Applicant (E.G. utility bill, phone bill, signed PO, Tax Exempt Letter, ORI Documentation, or other valid document).
    e. Acknowledgement of Applicant's IP (Internal Protocol) if Applicant has an onsite deployment of RMS. Queries/Requests from hosted Online RMS Applicants will all originate from the Caliber Nlets hosting center using an IP within the approved Caliber IP range.
    f. Acknowledgement of Applicant's responsibilities for Qualified Access and Security Requirements.
    g. Acknowledgement that Applicant will not further sell or otherwise transfer the information to any third party.
    h. Acknowledgement of Caliber's right to conduct an audit of Applicant's use and Applicant's obligation to cooperate and respond promptly.
2. Place a call to the verified main phone number for the Applicant as listed on the Application and asking to speak to the main contact listed on the Application to verify the contact is employed as an end user of the Applicant.
3. Utilize one of the three (3) nationwide credit bureau approved vendors to perform a physical site inspection of all Applicants utilizing a bureau approved inspection form to confirm the Applicant address and other information submitted in the Caliber Public Safety Embedded Accurint Query Application, Permissible Purposes Certification, and EULA. Copies of these documents will be provided to the selected site inspection vendor as required to complete the inspection.
4. Monitor Applicant's use of Caliber Public Safety Products and embedded Accurint queries. Caliber's agreement with Applicant Agencies enforce the security principle of "one user per Logon ID".
5. Verification that Applicant is not on the LexisNexis Reseller Alert List by logging onto https://learn.lexisnexis.com/reseller to download the Alert List.
6. Verification that Applicant is not on the Office of Foreign Assets Control ("OFAC") List (http://www.treas.gov/offices/enforcement/ofac/sdn/index.shtml).
7. Caliber will retain the Application, Permissible Purposes, site inspection report, documentation of credentialing steps, and executed customer EULA throughout the term of the agreement and for 5 Years after termination.

Caliber Public Safety Accurint Embedded Query Credentialing Program

SERVICE ACTIVATION

Upon successful completion of the above activities, Caliber application administrators will enable access to embedded Accurint Public Data Queries within Caliber Products and retain a copy of the excecuted EULA. Only users with the Applicant's agency will be granted access to the service.

1. Only Caliber administrators can provision access to embedded Accurint Public Data queries and configure the number of authorized end-users allowed to access the service.
2. Only authorized end-users within the Applicant's Agency having valid access to Caliber products can perform Accurint Public Data Queries. Access to Caliber products requires a valid Customer subscription, valid end-user id, and FBI Criminal Justice Information Services (CJIS) Security Policy conformant password.
    a. Caliber's agreement with Applicant Agencies enforce the security principle of "One end-user per Logon ID". Violation by Applicant Agencies may result in termination of services.
    b. Failed Logon attempts are tracked and will automatically lock/disable an end-user account after a specified number.