AURORA POLICE DEPARTMENT

Facial Recognition Accountability Report for
Rank One Computing Corporation's facial recognition service,
within LexisNexis' Lumen/AVCC software platform.

The Aurora Police Department submits this report pursuant to the requirements of Colorado Revised Statutes § 24-18-301 through 309. The Aurora Police Department ("APD") intends to activate the facial recognition functionality within the Lumen/AVCC software platform and to use it in support of law enforcement investigations.

The Aurora Police Department in Aurora, Colorado, intends to use the facial recognition functionality, facilitated by Colorado-based Rank One Computing, within LexisNexis' Lumen and Accurint Virtual Crime Center (AVCC) software platforms. Lumen/AVCC are software platforms that utilize the criminal justice information shared between the 140+ law enforcement member agencies of the Colorado Information Sharing Consortium (CISC). The facial recognition service within the Lumen/AVCC platforms are provided by Rank One Computing Corporation's (ROC) SDK version 2.2.1 algorithm. This software uses state-of-the-art facial recognition technology to find possible matches based on facial characteristics from a user-uploaded image to booking photos or other lawfully obtained images from CISC member agency records.

All use of facial recognition technology shall be for official law enforcement purposes only and considered law enforcement sensitive information. Per Colorado Revised Statute § 24-18-307, the Aurora Police Department will use this technology as an investigative lead only, with the full understanding that a potential match alone does not constitute probable cause.

I. Technical Description & Intended Use

The system compares a single user-uploaded "probe image" against a collection of lawfully available booking photographs and other images maintained by members of the CISC. Lumen/AVCC returns a ranked list of potential matches, each with a numerical confidence score. This score represents the likelihood of similarity, but it does not establish identity, positive identification, or probable cause.

Capabilities & Function
The Lumen/AVCC tool is designed to generate investigative leads by automating the process of comparing probe images against large volumes of criminal justice record images that would otherwise require manual review. Specifically:

- The algorithm creates mathematical templates from probe and candidate images to calculate similarity scores.

- The system uses machine-learning processes refined through operational testing, but results remain dependent on image quality and capture conditions (lighting, pose, occlusion, blur, glare, and resolution).
- Poor quality probe or candidate images may reduce accuracy.
- ROC SDK has been independently evaluated by the National Institute of Standards and Technology's (NIST) Facial Recognition Vendor Test (FRVT) and demonstrates low error rates (0.01%–0.00005%), though demographic variation exists.

The tool cannot and will not conduct real-time surveillance, live monitoring, or continuous tracking. It is strictly limited to after-the-fact investigative use.

Decision Making

Facial recognition results are investigative leads only and may not be relied upon as the sole basis for probable cause, arrest, or charging. APD personnel are required to:

- Review all results through meaningful human review by a trained investigator.
- Submit all identifications for peer review by another trained member prior to further use.
- Corroborate any potential match with independent evidence.

Intended Use and Benefits

The Lumen/AVCC facial recognition tool is intended to enhance the investigative abilities of the Aurora Police Department. This type of facial recognition technology automates the process necessary to locate potential matches between a probe image and thousands of criminal justice record images that would otherwise require a manual search by a human. The facial recognition algorithm will rank potential matches in a manner that allows for a simplified process of human review.

When provided a probe image to search against a collection of candidate images, Lumen/AVCC returns multiple results, sorted by the highest match score generated by the ROC SDK's facial recognition algorithms. Once Lumen/AVCC provides a list of results, a human investigator must review the results before making any determination of a possible match. A possible match determination may be used as an investigative lead that is treated in a similar manner as an anonymous tip. In particular, the investigative lead does not supply adequate probable cause to make an arrest without additional evidence. The intended benefit of using the Lumen/AVCC facial recognition service is to provide investigative leads that enhance follow-up inquiries and increase the likelihood of solving crimes that might otherwise remain unsolved.

In comparable use by the New York City Police Department (NYPD) since 2011, the NYPD has successfully used facial recognition to identify suspects whose images have been captured by cameras at robberies, burglaries, assaults, shootings, and other crimes. In 2019 alone, the Facial Identification Section received 9,850 requests for comparison and identified 2,510 possible matches, including possible matches in 68 murders, 66 rapes, 277 felony assaults, 386 robberies, and 525 grand larcenies, with no known instance in which a person was falsely arrested based on a facial recognition match.[1]

The use of facial recognition software will assist the Aurora Police Department with:

- Increasing public safety and improving state, local, and national security.
- Minimizing the threat and risk of injury to specific individuals.

[1] https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, and health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Reducing the opportunities for bias and prejudice to impact the criminal justice process.
- Protecting the integrity of criminal investigations, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to the police department.

Data Inputs and Generation

The Lumen/AVCC facial recognition tool uses the following types of data inputs:

- User submitted probe images collected during criminal investigations and associated information identifying the purpose of the search (such as case number, crime time, and justification for use).
- The candidate facial image data is primarily jail booking photos or other lawfully obtained images that are collected by the CISC from its member agencies who elect to share images.

The Lumen/AVCC facial recognition tool generates a template of each facial image, which is a mathematical model of the unique subject which may be compared to templates generated from other images to produce a match score. For each facial image, the tool also generates metadata including pitch, yaw, image quality estimations and facial analytics like age, gender, geographic origin, emotion, facial hair, glasses and mask estimations.

II. Data Management, Training and Use Policy

The Aurora Police Department will follow statutory requirements described in Colorado Revised Statutes § 24-18-301 through 309, in conjunction with an approved department policy. As such, the department will follow the below guidelines regarding data management, training and the authorized use of the facial recognition service.

Data Minimization

The features and functions of the Lumen/AVCC facial recognition tool effectively reduce the risk of inadvertent access to data by APD personnel. The Lumen/AVCC facial recognition tool searches only criminal justice records available to CJIS-certified law enforcement personnel of CISC member agencies. The criminal justice records available in the facial recognition tool are subject to the retention policies of the owner agencies.

Data Integrity and Retention

The designated Facial Recognition Administrator will be responsible for overseeing all Lumen/AVCC facial recognition tool permissions for the Aurora Police Department. Access to this tool will be restricted to a limited number of trained investigative and analytical personnel with individual accounts. The Facial Recognition Administrator will have the capability to audit and review any, and all usage of this facial recognition tool by any member of the department. The audit will include all user activity, such as user log ins and log outs, what commands were issued to the system, and what records or files were accessed.

All information obtained from the Lumen/AVCC facial recognition tool by any member of the police department will be collected in a formal report and retained in accordance with guidelines set forth in the record management system.

Without the express permission of APD, or as required by law, such as a judicial order, LexisNexis employees will not review APD search history within the Lumen/AVCC facial recognition tool, ensuring that sensitive investigative data will remain confidential.

All information available within the Lumen/AVCC investigative platform, including the facial recognition tool, is purged according to the retention schedule and policies set by the owner agency. For example, any information made available to other CISC member agencies by APD is purged from the Lumen/AVCC investigative platform when its retention expires inside APD's record management system.

Usage Rules and Requirements

Access to the Lumen/AVCC facial recognition tool within the Aurora Police Department will be strictly limited to set number of personnel who are trained in its use. Each authorized user will have individual credentials, and the Facial Recognition Administrator will oversee access approvals, maintain user records, and conduct audits to ensure policy compliance. Operators are responsible for reviewing the quality and suitability of probe images prior to initiating a search, with careful consideration of factors such as pose, clarity, illumination, and image resolution. Original probe images must remain unaltered; any enhancements must be applied only to copies, with documentation identifying the type of change, date, time, and operator. All comparisons are subject to human review, and results must undergo peer verification by another trained member prior to investigative use.

Every search conducted in the facial recognition system will be fully documented, including the operator's name, date and time of the request, case number, and the stated purpose of the search. This information will be logged automatically and maintained for review and auditing. Regular audits will be conducted to monitor usage, identify error rates, and ensure that no misuse or irregularities occur.

The Aurora Police Department will comply with all Colorado statutes, department directives, and any Memoranda of Understanding governing participation in shared databases. The Department does not own or permanently retain images accessed for searches; instead, candidate images remain subject to the retention policies of the source databases. Case-related results will be retained in accordance with Department policy. Pursuant to Colorado Revised Statute § 24-18-303, the Department will disclose the use of facial recognition technology to a criminal defendant in a timely manner prior to trial.

To ensure accountability and safeguard individual rights, the Department prohibits the use of facial recognition for real-time surveillance, continuous monitoring, or the creation of independent facial recognition databases. The Facial Recognition Administrator will ensure compliance with state-mandated reporting requirements, including annual monitoring of accuracy, error rates, and potential demographic bias. If error rates exceed one percent, or if evidence of disparate impact arises, the Department will suspend use until corrective measures are implemented. These rules are designed to balance the investigative value of facial recognition technology with the protection of privacy, civil rights, and public trust.

Data Security

Facial recognition data is stored securely on CJIS-compliant Lumen/AVCC servers, and access is limited to individual authorized users within Lumen/AVCC.

Lumen/AVCC is web-based software and not an application which needs to be downloaded to any City of Aurora computers. Any records exported by Aurora Police Department members shall be immediately uploaded to the department's record management system (Versadex). Versadex is CJIS compliant and maintained by the City of Aurora's Information Technology department.

Training Procedure

Training will be provided by the Aurora Police Department to all authorized users of facial recognition services. This training will be arranged and documented by the Facial Recognition Administrator and account access will not be created or provided until training has been completed.

Training will cover both the use of facial recognition software/technology as well as a specific review and acknowledgment of all elements of related department policy.

Per Colorado Revised Statute § 24-18-305, the training will at a minimum include:

- The capabilities and limitations of the facial recognition service.
- Procedures to interpret and act on the output of the facial recognition service; and
- The meaningful human review requirement for decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals.

The use of the Lumen/AVCC facial recognition tool will include specific training that includes the following:

- the authorized user shall enter the required information to support the authorized use of facial recognition satisfying an official law enforcement purpose,
- a lawfully obtained probe image of a subject meeting the required authorized use is uploaded to the system,
- the software automatically compares the probe image to candidate images within the repository,
- results of the comparison are returned and provide a potential investigative lead.

Updated training shall be identified with any policy revisions or updates in facial recognition software.

III. Accuracy and Impact

Testing Procedure

In accordance with Colorado Revised Statute § 24-18-304(4), Rank One Computing submitted the ROC SDK for testing in the following series of the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) Ongoing:

1:1 Verification:	*https://pages.nist.gov/frvt/html/frvt11.html*
1: N Identification:	*https://pages.nist.gov/frvt/html/frvt1N.html*
Quality Assessment:	*https://pages.nist.gov/frvt/html/frvt_quality.html*
Demographic Effects:	*https://pages.nist.gov/frvt/html/frvt_demographics.html*
Paperless:	*https://pages.nist.gov/frvt/html/frvt_paperless_travel.html*

Test Results

Rank One Computing's SDK facial recognition algorithm was submitted to the National Institute of Standardization and Technology (NIST) Face Recognition Technology Evaluation (FRTE) for 1:1 Verification. In that test, ROC's SDK facial recognition algorithm ranked No. 6 in the world out of 404 total entries.[2]

	FALSE NON-MATCH RATE (FNMR)							
	Constrained, Cooperative						Unconstrained, Non-Coop	
Algorithm	Gallery	VISA	MUGSHOT	MUGSHOT	VISA	VISA Yaw≥45	BORDER	BORDER
	Probe	VISA	MUGSHOT	MUGSHOT ΔT≥12 YRS	BORDER	BORDER°	BORDER	KIOSK
	Date	FMR = 0.000001	= 0.00001	= 0.00001	= 0.000001	= 0.000001	= 0.000001	= 0.00001
qazsmartvisionai-004	2025-07-18	-	0.002(1)	0.002(3)	0.0014(1)	0.003(2)	0.0028(1)	0.0337(1)
viante-002	2025-06-17	-	0.0025(52)	0.0024(29)	0.0015(2)	0.0028(1)	0.0029(2)	0.0349(2)
recognito-001	2023-09-27	0.0007(2)	0.0021(4)	0.0022(14)	0.0016(3)	0.007(15)	0.0662(202)	0.1047(123)
cloudwalk-mt-007	2023-02-21	0.0007(1)	0.0023(23)	0.0019(1)	0.0016(4)	0.0036(3)	0.0032(4)	0.0394(9)
paravision-018	2025-06-12	-	0.002(2)	0.002(4)	0.0016(5)	0.0038(4)	0.0034(7)	0.0375(5)
roc-019	2025-07-21	-	0.0021(10)	0.0021(8)	0.0016(6)	0.006(11)	0.0031(3)	0.038(6)

Bias and Inaccuracy

In the NIST Demographic Effects series the ROC SDK algorithm ranked 11th worldwide (out of 597 entries) across all 70 sub-populations of the NIST test data, with the lowest scoring demographic being West African females aged 65-99 years old (0.01061% false match rate).[3] The potential for technological bias and inaccuracy is further mitigated through required meaningful human review of each potential match and secondary peer review by another trained member. Final supervisory approval is also required before any investigative lead is forwarded for follow-up

Civil Rights Impact

The Aurora Police Department recognizes the importance of safeguarding civil rights, civil liberties, and privacy in the use of facial recognition technology. To address these concerns, multiple layers of oversight and human judgment are built into every stage of the process. The Lumen/AVCC system does not make identifications or determinations of guilt; rather, it generates a ranked list of possible matches based on a submitted probe image. These results are reviewed by trained investigators, who are required to apply their professional expertise to determine whether any candidate represents a possible match. No investigative action may proceed without additional independent evidence, and a possible match may only serve as an investigative lead, comparable to an anonymous tip.

Probe images are drawn exclusively from lawfully obtained criminal justice records, such as arrest booking photographs, and are never collected from unauthorized sources. To further protect against potential bias or disparate impact, every authorized user must input a valid case number and specify the type of crime under investigation prior to initiating a search. This requirement affirms that the technology is being used exclusively to investigate crimes that have already occurred and not to monitor lawful activities, conduct "fishing expeditions," or track individuals engaged in constitutionally protected activities. Compliance with this rule will be verified through routine audits of user inputs and system usage.

[2] https://pages.nist.gov/frvt/html/frvt11.html

[3] https://pages.nist.gov/frvt/html/frvt_demographics.html

The Aurora Police Department also maintains strict adherence to APD Directive 08.32: Bias-Based Policing, which prohibits investigative activity based in whole or in part on an individual's actual or perceived race, ethnicity, gender, national origin, language preference, religion, sexual orientation, gender identity, age, or disability. Investigations may only rely on demographic descriptors when they are part of a reliable, suspect-specific description that also includes non-demographic identifying characteristics.

In addition, APD's Facial Recognition Policy requires investigators to document every search, including the requestor's name, date, time, case number, and purpose. This ensures transparency, accountability, and a record of lawful use. Audit logs will be reviewed to detect any misuse, and violations of policy will be subject to disciplinary action.

Independent testing conducted by NIST has demonstrated that the ROC SDK algorithm used within Lumen/AVCC performs with high levels of accuracy across demographic groups, with measured performance exceeding 99% accuracy in the FRVT Demographic Effects program. While no technology is free from error, these results indicate that the risk of disparate impact on marginalized communities is extremely low. Importantly, any potential error is further mitigated by the requirement for human review, corroborating evidence, and supervisory oversight before any investigative or enforcement action is taken.

Through these safeguards, the Aurora Police Department is committed to ensuring that the use of facial recognition technology supports public safety while protecting civil rights, civil liberties, and the trust of the community.

Public Feedback

The Aurora Police Department will seek approval from the Aurora City Council prior to the implementation and utilization of the Lumen/AVCC facial recognition tool. As is required by Colorado Revised Statute § 24-18-302, consideration and the opportunity for public comment will be heard at a Public Safety Committee Meeting, Council Study Session, and Council Regular meeting should the item be moved forward at each meeting respectively.

Public comments and feedback on the use of facial recognition technology can be submitted through an online form available in the Facial Recognition section of the Aurora Police website. All feedback will be reviewed and addressed in accordance with agency procedures.