

Mixon, Benjamin

From: 86806-47086858@requests.muckrock.com
Sent: Wednesday, January 29, 2020 11:09 AM
To: Mixon, Benjamin
Subject: Georgia Open Records Act Request: FOIA - Cobb County/Marietta PD, GA - Flock Safety Documents (Marietta Police Department)

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Marietta Police Department
ORA Office
240 Lemon St NE
Marietta, GA 30060

January 29, 2020

To Whom It May Concern:

Pursuant to the Georgia Open Records Act, I hereby request the following records:

All documents pertaining to Flock Safety (<https://www.flocksafety.com>) license-plate-reader hardware and/or software. Documents being requested here should include - but are not limited to - the following:

- Invoices, receipts, and/or requests for the purchase of any Flock Safety product/service
- MOUs from Flock Safety
- Brochures or product/service specifications regarding Flock Safety
- Privacy and/or retention policies regarding Flock Safety product/services
- Any/all manuals regarding Flock Safety product/services
- Guidelines mentioning Flock Safety product/services
- Bulletins mentioning Flock Safety product/services
- Briefings mentioning Flock Safety product/services
- Any/all digitally disseminated publications from your agency mentioning Flock Safety product/services

I am confident there are documents relevant to this request based on public literature and broadcast news video describing the use of the company's products by your agency: <https://www.flocksafety.com/police>

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 3 business days, as the statute requires.

Sincerely,

J Ader

Filed via MuckRock.com

E-mail (Preferred): 86806-47086858@requests.muckrock.com

Upload documents directly:

https://accounts.muckrock.com/accounts/login/?url_auth_token=AABAGTdHW11E21ufNOIxUNh8GXs%3A1iwpth%3An_QABMkN_ONKj-lmQs9YCdrWbsA&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fmarietta-police-department-12060%252Ffoia-cobb-countymarietta-pd-ga-flock-safety-documents-marietta-police-department-86806%252F%253Femail%253DBMixon%252540mariettaga.gov

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News

DEPT MR 86806

411A Highland Ave

Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



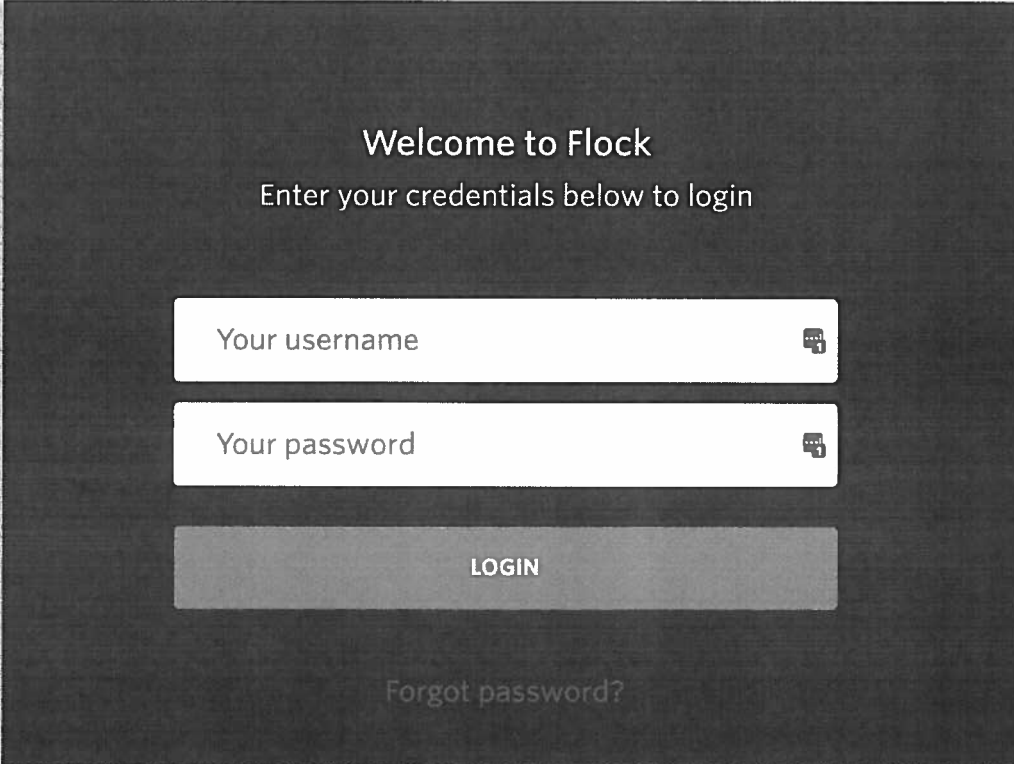
The slide features a large, light gray circular graphic in the center, which contains a white silhouette of a bird in flight. The title text is centered over this graphic.

Flock Safety Admin

Overview

Login Screen

Each user will receive an email from hello@flocksafety.com with login credentials to sign in. (Login credentials cannot be shared in this tool)

A dark-themed login screen mockup. At the top, it says "Welcome to Flock" followed by "Enter your credentials below to login". Below this are two white input fields: "Your username" and "Your password", each with a small icon on the right. Under the password field is a grey "LOGIN" button. At the bottom, there is a link that says "Forgot password?".

Welcome to Flock

Enter your credentials below to login

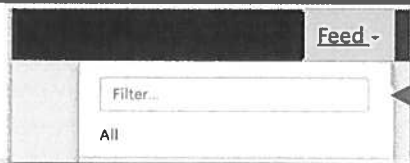
Your username

Your password

LOGIN

Forgot password?

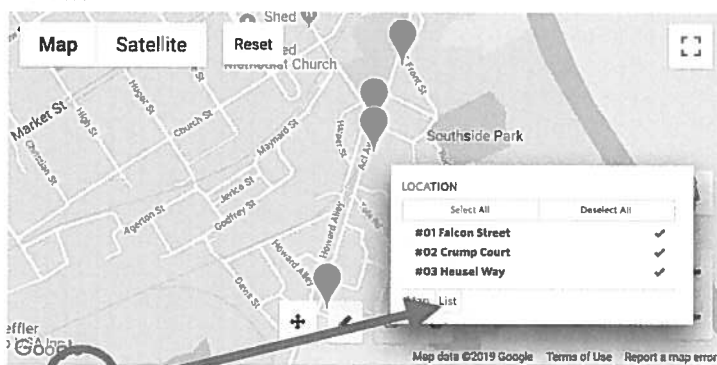
Feed



To review footage, select the “Feed” tab and filter on the desired network if applicable.

Bailey Demo Cam powered by flock safety

LOCATION



FROM

Mar 1 2019

9:00am

TO

Mar 1 2019

11:00am

OBJECTS

Vehicle

Bicycle

Animal

Person

☒ INCLUDE UNPROCESSED

SUBMIT SEARCH REQUEST

Filter your search by camera in the map list view shown above & submit search request.

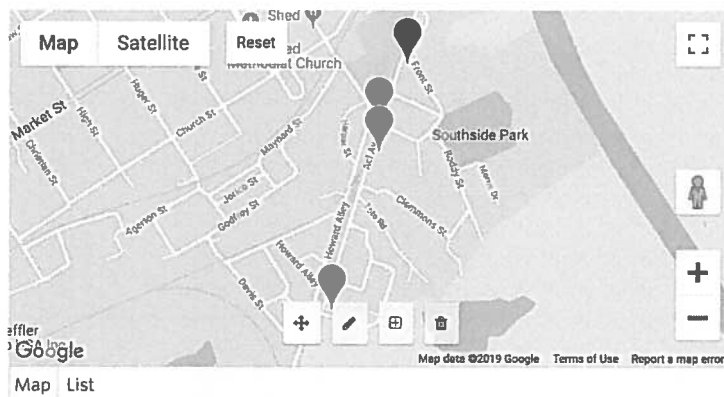
Additionally filter your search by date, time or objects & submit search request.

Unprocessed images are images that haven't been labeled yet.

Feed

Bailey Demo Cam powered by flock safety

LOCATION



FROM

Mar 1 2019 9:00am

TO

Mar 1 2019 11:00am

OBJECTS

Vehicle	Bicycle	Animal	Person
Enter License Plate			
Build	SED	Car	
Role		Truck	
Color		Bus	
Residents		Motorcycle	

SUBMIT SEARCH REQUEST

Narrow down your search by filtering for a vehicle's license plate, build or color.


Partial tag numbers are searchable with characters in order (eg. ABC will return on a search for ABC123, 123ABC, 1ABC2, etc)

Also search for bicycles, animals or persons and submit search request.

Feed

1. Car (100.0%)

- License Plate: GA CFE5208 (87.0%)
- Color: White (99.6%)
- Seen 4 of the last 21 days



Bailey Demo Cam - Crump Cam

4/5/2019 13:35:06 EDT

The time-stamp of when the image was taken will be shown on the right-hand corner of the image.

Objects and license plates captured by the camera will be labeled on the left-hand side of the screen.

The percentages identify our confidence rate of the objects we've detected.

Feed

1. Car (100.0%)

- License Plate: GA CFE5208 (87.0%)
- Color: White (99.6%)
- Seen 4 of the last 21 days



At any given time, you can “Flag” the image if the information on the left hand-side of the image is detected incorrectly.

Select the “Play” icon to view the burst of images in motion.

Select the magnifying glass icon to enlarge the picture, scroll through each frame and download the image.



Marietta Police Department

240 Lemon Street, Marietta, Georgia 30060 Telephone 770-794-5300 Fax 770-794-5301

Dan Flynn, Chief of Police

TRANSMITTAL MEMORANDUM

TO: Bill Bruton, City Manager
City of Marietta

FROM: Dan Flynn, Chief
Marietta Police Department

DATE: July 11, 2019

SUBJECT: ALPR Flock Camera Locations

The general locations for the Flock License Plate Readers were selected by four of our five Majors. These Majors are responsible for the four zones the City is divided into (the fifth Major is not assigned a zone). The Majors decided collectively to "bracket the city" with license plate readers in an effort to further criminal investigations and increase solvability factors.

These twelve to fourteen locations were then sent to Lt. Mixon (Technology Manager) who coordinated with Flock. The formed team set up a time to consider each location and pick the best ten. From the general locations that were selected by the Majors, Lt. Mixon and Flock representation considered lanes of travel, proper angles for the cameras to read tags, as well as the amount of sunlight each location received throughout the day. Lt. Mixon narrowed our scope from general locations to specific ones, at which time we submitted them to the Street Department for approval.

The ten chosen locations are:

- Church St (SB) Median
- Allgood Rd (WB)
- Atlanta Rd (NB)
- Fairground St (SB)
- Fairground St (NB)
- Cobb Pkwy (NB)
- Powder Springs (NB)
- Roswell Rd (WB)
- Northwest Pkwy (EB)
- Whitlock Ave (EB)

***Pictures can be provided*

"Policing With A Vision"

FLOCK GROUP INC.

PO Box 207576

Dallas, TX 75320-7576

**SAAS SERVICES AGREEMENT
ORDER FORM**

This Order Form together with the SaaS Terms (as defined herein) describe the relationship between Flock Group Inc. ("Flock") and the customer identified below ("Customer") (each of Flock and Customer, a "Party"). This order form ("Order Form") hereby incorporates and includes the "Terms and Conditions" located at <https://www.flocksafety.com/legal/terms-and-conditions> (the "SaaS Terms") which describe and set forth the general legal terms governing the relationship (collectively, the "Agreement"). The SaaS Terms contain, among other things, warranty disclaimers, liability limitations and use limitations.

The Agreement will become effective when this Order Form is executed by both Parties (the "Effective Date").

Customer: Marietta Police Department	Contact: Benjamin Mixon
Address: 240 Lemon St NE, Marietta, GA 30060	Email: bmixon@mariettaga.gov
	Phone: (770) 794-5386
	Initial Term: 13
Usage Fees: \$20000 per year (the "Payment Period")	Renewal Term: 12
Number of Cameras: 10	
Installation Fee (one-time): \$0	

By executing this Order Form, Customer represents and warrants that it has read and agrees all of the terms and conditions contained in the SaaS Terms located at <https://www.flocksafety.com/legal/terms-and-conditions>.

The Parties have executed this Agreement as of the dates set forth below.

Flock Group Inc <i>Bailey Quintrell</i> By: _____ Name: Bailey Quintrell Title: Head of Public Safety Date: 04/08/2019	Customer Name: <i>Benjamin Mixon</i> By: _____ Name: Ben Mixon Title: Lieutenant Date: 04/09/2019
--	---

Flock Group Inc.

**Order Form
613647607**

EXHIBIT A

Statement of Work

Installation Services includes the following:

Installation of Flock Safety cameras on existing poles or on Flock-Supplied 14ft poles.

Installation of Flock signage (if desired)

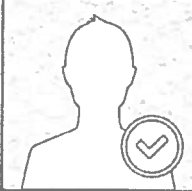



Flock Group Inc.

**Order Form
613647607**

Signature Certificate

Document Ref.: PCNRZ-8PTZT-JBEXA-2CFYP

Document signed by:

	Bailey Quintrell Verified E-mail: bailey@flocksafety.com 50.224.116.3 09 Apr 2019 03:16:20 UTC	
	Benjamin Mixon Verified E-mail: bmixon@mariettaga.gov 88.158.165.250 09 Apr 2019 12:08:48 UTC	

Document completed by all parties on:

09 Apr 2019 12:08:48 UTC

Page 1 of 1



Signed with **PandaDoc.com**

PandaDoc is the document platform that boosts your company's revenue by accelerating the way it transacts.



MARIETTA POLICE DEPARTMENT
STANDARD OPERATING PROCEDURE

SUBJECT Photograph/Video/Audio Recording Equipment	EFFECTIVE DATE May 16, 2019	SOP # P015
REFERENCE Photograph/Video/Audio Recordings; Videotapes; Photograph/Video/Audio Equipment and Hardware; Data Storage; Digital Media Viewing Software		
SPECIAL INSTRUCTIONS		
DISTRIBUTION All Sworn & Non-Sworn Personnel		# PAGES 12

I. PURPOSE

The purpose of this policy is to provide guidelines for the use of department authorized photograph/video/audio recording equipment, and the disposition of videotape, digital photographs, digital video/audio recordings, and metadata these devices collect.

II. POLICY

This policy applies to all personnel operating department authorized photograph/video/audio recording systems, to include in-car video camera systems, body-worn cameras (BWCs), posted security cameras (PSCs) and automated license plate readers (ALPRs). This equipment shall always be used in conformance with Georgia law as well as the policies and procedures of the City of Marietta.

III. APPLICATION

- A.** The routine use of authorized photograph/video/audio recording equipment is for the purpose of recording specified interactions between police personnel and the public and to collect evidence for criminal procedures. The use of the photograph/video/audio recording equipment will allow for increased accuracy in documentation of police-public contacts, arrests, and critical incidents, as well as to enhance accuracy with police reports and courtroom testimony.
- B.** Videotapes, digital photographs, and digital recordings shall be treated as evidence. Employees are prohibited from altering, destroying, or any unauthorized viewing of these tapes and digital recordings.

- C. Videotapes, digital photographs, and digital recordings are the property of the Marietta Police Department and shall be governed by policies dealing with property and evidence.
- D. Officers and supervisors will be trained on the use of the in-car video camera systems and the BWCs. This training may be provided by the manufacturer of the product, the vendor of the product or from City of Marietta personnel trained in the use of the equipment. Additional training may be required at periodic intervals to ensure continued effective use and operation of the equipment, proper calibration and performance, and to incorporate changes, updates, or other revisions in policy.

IV. PROCEDURES

Officers and civilian personnel designated to use video/audio recording equipment shall adhere to the following procedures when utilizing video/audio equipment:

A. In-Car and Interview Room Video/Audio Camera Equipment

- 1. Unless provided by the vendor, installation and maintenance shall be performed by authorized service personnel. Alterations of the installed system by unauthorized personnel is prohibited.
- 2. Prior to each shift or interview, officers and PTOs shall determine whether their in-car or appropriate interview room video/audio equipment is functioning satisfactorily. Officer and PTOs will bring any problems at this time or any other times to the attention of their immediate supervisor as soon as possible. Any equipment errors shall be documented on a vehicle maintenance form or through IT HelpDesk request.
- 3. Prior to each shift, officers and PTOs, except those driving their assigned PPVP, will log into the in-car video/audio equipment and log out at the end of the shift.
- 4. The in-car video/audio equipment is automatically activated when emergency lights and/or siren are turned on. The interview room video/audio equipment is activated/deactivated by manually pressing the record on/off button outside of the interview room.

Note: It is each user's responsibility to ensure the video/audio equipment has activated automatically or manually initiated.

5. Officers and PTOs without properly functioning in-car systems will manually activate the in-car video/audio equipment when necessary to record other events, situations, and circumstances, including but not limited to, armed encounters, acts of physical violence, field interviews, suspicious person checks, civilian transports and felonious conduct.
6. When asked, officers will inform citizens that audio/video recording equipment is in use. If applicable, Officers and PTOs shall at all times wear the voice link transmitters or other patch microphones assigned to be used with the in-car recording devices. Officers and PTOs shall at all times audio/video record: traffic stops, pursuits, suspicious person(s) checks, civilian transports and accident investigations. No officer or PTO will disconnect or turn off their assigned microphone when performing any of the above-mentioned duties. The audio/video recording shall be a complete and accurate record of the officer's and PTO's activities.
7. When applicable, digital audio recorders will be assigned to personnel and will be activated in the interview rooms as a back-up audio recorder. All interview audio files will be digitally attached to its respective case file within the records management system.
8. In-car and interview room video/audio recordings will be uploaded automatically to a secured server. Administrator access to the server and its digital media shall be limited to the persons designated by the Deputy Chief of Support Services.
9. In-car cameras may capture images that are in plain view when cameras are facing a residence or business. If needed, a search warrant shall be obtained.
10. If a PPVP vehicle has a malfunctioning recording system, the officer will utilize a spare vehicle when on duty. Vehicles with malfunctioning recording systems will only be utilized if no other vehicle is available.

B. Body-Worn Cameras (BWCs)

1. BWCs will be worn by officers, when available, up through the rank of Lieutenant, while on-duty and dressed in uniform. Civilian personnel designated by the Chief of Police shall also wear BWCs, when available, while on-duty and dressed in uniform. All sworn personnel, through the rank of Major, working a secondary employment job, in accordance with

S.O.P. A050, will also wear a BWC and comply with part IV.B.5. of this policy.

2. BWCs will be worn on approved duty uniforms using the manufacturer's designed holster/clip and in a location that facilitates an optimum recording field of view. Officers will ensure the BWC lens is not covered by any article of clothing or other material.
3. Prior to each shift, personnel designated to wear a BWC shall determine whether their assigned BWC is functioning satisfactorily and is fully charged. Any problems will be brought to the attention of their immediate supervisor as soon as possible so a replacement unit may be issued or other remedy applied.
4. Personnel designated to wear a BWC may record in any place when acting within the lawful performance of his or her official duties, see O.C.G.A. 16-11-62 (2) (D).
5. Personnel designated to wear a BWC will make every reasonable effort to activate their BWC prior to initiating, or as soon as practical after initiating, the following actions during the course of their official duties:
 - a) All enforcement encounters where at least reasonable suspicion that the person(s) encountered has committed, is committing, or may be involved in criminal activity. This includes, but is not limited to:
 - i. Detentions, vehicle stops, pedestrian stops, "knockand-talks", field interviews, and consensual encounters.
 - ii. Arrest or attempts to effect arrest.
 - iii. Prisoner/arrestee exchanges between officer and officer/PTO or PTO and Jail/Court.
 - iv. Enforcement encounters where there is reason to believe that a citation may be issued.
 - v. All incidents involving use of force.
 - vi. Any public interaction, regardless of context, that escalates and becomes adversarial.
 - vii. Service of search or arrest warrants.
 - viii. Suspect statements.
 - ix. Witness/victim statements (Except for circumstances stated in section IV.B.6.i.).
 - x. Pursuits (when practical).
 - xi. Response to complaints.
 - xii. When backing up another officer involved in one of the above stated activities.

6. BWCs shall not be activated to record:

- a) Intelligence gathering communication between an officer(s) and confidential informant(s).
- b) To surreptitiously record any city personnel or other government personnel without their consent, court order, or lawful permission by the Chief of Police or designee for the purposes of criminal investigation (ref S.O.P. A030.IX.10.33, Photographs and Digital Recordings).
- c) When on a break or engaged in personal activities.
- d) In any location where individuals have a reasonable expectation of privacy, such as a restroom or locker room, except in performance of lawful duties.
- e) Tactical briefings or other operational briefings which may discuss safety and security procedures.
- f) Strip searches.
- g) Doctor or lawyer's offices, except in performance of lawful duties.
- h) Medical or hospital facilities, except in performance of lawful duties.
- i) A victim, witness, or confidential informant who requests that they not be recorded as a condition of cooperation and the interests of justice requires such cooperation.

7. Personnel are not required to activate the camera system during routine, incidental contact with a citizen (i.e. giving navigational directions, civic related information, town hall meetings, etc.). Also, officers will not be required to activate or deactivate their BWC based solely on the requests or demands of a citizen, but rather rely on their training and this policy to guide their use of the BWC.

8. The BWCs will remain activated until the recorded event is concluded in order to ensure the integrity of the recording. However, the recording may be suspended or terminated under certain circumstances:

- a) When an officer/PTO is at a scene or expected to be at a scene for an extended period of time. This may only be done after the scene is secured and there are no citizen interactions relevant to the investigation. (Examples of these situations would be an officer posted on a perimeter of a secured crime scene or an officer or PTO standing-by

at a detention facility or medical center with no direct contact with the detainee/arrestee.)

- i. If during this time there is incident-relevant citizen/detainee contact, the officer/PTO will activate the BWC.
- b) When an officer/PTO engages in conversations with individuals with whom they have a privileged relationship (e.g. spouse, attorney, doctor, clergy, etc.).
- c) When an officer is at a secure crime scene requiring the BWC to be used to capture photographs for evidence recording/processing.
 - i. If during this time there is incident-relevant citizen/detainee contact, the officer/CST will activate the BWC to record video & audio.

Officers and PTOs should exercise sound judgment when deciding when to suspend or terminate a BWC recording. Anytime a recording is suspended or terminated prior to the end of the incident/citizen encounter, the reason(s) should be documented both on the BWC recording and in the subsequent incident report. If no incident report is generated, then the reasons(s) should be documented on the citation, field interview card, or accident report.

- 9. If an officer or civilian personnel designated to wear a BWC fails to activate the BWC, fails to record the entire contact, or interrupts the recording, other than for reasons stated in section IV.B.6. of this policy, the officer will document why a recording was not made, interrupted, or terminated and forward the documentation to his/her supervisor. The supervisor will maintain these documents within their shift/unit electronic folder on the V-Drive and forward a copy to the Technology Management Lieutenant.
- 10. When asked, officers and civilian personnel designated to wear a BWC will inform citizens that the BWC is activated. If the citizen does not ask, officers and civilian personnel may choose to tell the citizen that the BWC is activated.
- 11. Citizens shall not be permitted to review photographs or recordings at the scene.
- 12. If not done automatically via in-car system, all files will be securely uploaded into the approved digital media repository periodically

throughout the officers' and civilian personnel's shift at the secondary upload location(s), but no later than the end of each shift. Each file shall contain information related to the date, BWC identifier, and assigned user.

13. Officers and civilian personnel will classify BWC media in accordance with section V of this policy. In addition, BWC media will include, but not be limited to, metadata within the notes field such as case number and type of incident.
14. BWCs may capture images that are in plain view when activated within a residence or business. If needed, a search warrant shall be obtained.
15. Officers involved in a use of deadly force situation will be permitted to review BWC recordings prior to submitting to interviews or rendering statements to supervisors or investigators.

C. Posted Security Cameras (PSCs)

Posted security cameras shall be placed in locations reporting a significant number of crimes, violent crimes, repetitive crimes or those locations where events such as parades / demonstrations, festivals, celebrations, or cultural events pose an increased public safety risk.

1. Officers will only utilize approved PSCs devices, as determined by the Chief of Police, or his designee.
2. Requests for a PSC to be used may be verbal or written and forwarded to the appropriate Major for approval prior to deployment.
3. Installment, deployment and maintenance of PSC equipment will be completed by authorized trained personnel.
4. Access to posted security cameras shall be by individual user name and password. User names and passwords shall not be shared or transmitted to any other persons.
5. PSCs shall not be pointed inside or within areas where there is an expectation of privacy, such as within a private business or residence, without a search warrant.
6. Recordings from PSCs with evidentiary value will be maintained by the investigating officer and placed into evidence or attached to the investigator's electronic case file within the department's Report

Management System. All non-evidentiary recordings will be disposed of by the investigating officer upon completion of the investigation.

D. Automated License Plate Reader (ALPR)

A vehicle mounted electronic device that scans the immediate area and automatically compares license plates read to lists of wanted vehicle data via a secure network.

1. Officers driving ALPR equipped vehicles will make reasonable attempts to utilize the system while on patrol.
2. ALPR alerts are not probable cause for action. However, alerts should be considered as reasonable articulable suspicion to further investigate and verify information.
3. When the ALPR alerts the officer of a potential "hit", the officer will make reasonable attempts to verify the validity of the information before initiating a traffic stop.
4. Officers will use proper due regard to traffic safety in any traffic maneuvers required to intercept the target vehicle.
5. If a "hit" is determined to be invalid, or out of date, the officer will notify the originating agency that their NCIC record needs to be updated or purged.
6. ALPR historical data will be used for official law enforcement related investigative purposes only.
7. ALPR administrators will have access to audit information showing who is performing queries of the system.
8. Historical data is stored on the servers of vendor and is password protected.
9. To provide mutual aid, the department will only share its ALPR historical data with other law enforcement agencies to assist investigations.
10. Use of the historical data for personal reasons is prohibited.

11. All officers operating vehicles with ALPR systems will receive training in the use of the system to include how to aim the cameras, verify "hits", correct inaccurate reads, and accessing historical data.
12. Officers and detectives accessing historical data via the software provided will receive training prior to being provided a password.
13. ALPR historical data shall be destroyed no later than 30 months after such data was originally collected, unless such data is the subject matter of a toll violation or for law enforcement purpose.
14. ALPR administrators will be responsible for handling updates from other agencies regarding any department historical data.

E. SMILE Program (Systems in Marietta Intersecting with Law Enforcement)

1. The Marietta Police Department, partnering with the community, has developed an inventory of video cameras throughout the city. This partnership is completely voluntary on behalf of the camera owner and applies to both commercial and residential cameras.
2. Video collected from this partnership will be used solely for investigative purposes and only with the expressed consent of the owner of the video footage in question. Video will not be requested for any other purpose. Video will be handled in accordance with established department policy A060.
3. Enrollments will be collected via an online link, accessible through the City's website, and maintained by City of Marietta IT staff in conjunction with the Technology Lieutenant. The information gathered will be stored in the mapping software, will be protected, and will only be accessible by approved personnel.
4. Video obtained from this database, for evidentiary reasons, will be maintained then destroyed based on evidentiary and open record retention guidelines established by the State and Marietta PD policy.
5. Administrators for the site will be created and maintained by the Technology Lieutenant, in conjunction with City of Marietta IT staff. An example of officers who will have access are, but not limited to: Detective Supervisors, Support Services Lieutenant, Uniform Patrol Supervisors, CIU Supervisor, and those authorized by the Chief of Police.

6. An annual audit of enrolled cameras will be conducted by the Technology Lieutenant.

V. CLASSIFICATION OF INTERVIEW ROOM, POLICE IN-CAR, AND BODY WORN CAMERA MEDIA AND RETENTION SCHEDULE FOR RECORDED POLICE MEDIA

When personnel activate their BWC, in-car camera, or an interview room camera in accordance with this policy, upon deactivation of the recording the user will classify the digital media with one of the following classifications that most appropriately applies to the content:

A. Enforcement

This classification will be used for any: detention; vehicle stop; pedestrian stop; “knock-and-talk”; field interview; consensual encounters resulting in detention or arrest; arrest or attempts to effect arrest; prisoner/arrestee exchanges between officer and PTO, or PTO and Jail/Court; encounters where a citation is issued; all incidents involving use of force; service of search or arrest warrants; captured vehicular accidents; pursuits; crime scene photographs. (Retain media for a minimum of 30 months per the Georgia Retention Schedule for Local Governments. Media will be maintained in the City of Marietta approved repository system).

B. Non-Enforcement

This classification will be used for any photograph or recording which captures media not pertinent to criminal or civil prosecution. Examples would include, but not be limited to: accidents which result in no citation or arrest; business disputes that peaceably conclude through officer mediation; contact person calls; disabled motorist assists; unintentional recordings, etc. (Retain media for a minimum of 180 days per the Georgia Retention Schedule for Local Governments. Media will be maintained in the City of Marietta approved repository system).

C. Detective Interview or Homicide Interviews

This classification will be used for any interview room recordings which captures interviews conducted by Investigative Services personnel or pertains to other in-depth criminal investigations. (Retain media for a minimum of 10 years for detective interviews and 99 years for homicide interviews to ensure they are kept through court adjudication. Media will be maintained in the City of Marietta approved repository system).

When classifying video, officers and civilian personnel will indicate at minimum the case number or CAD call number in the metadata notes

video/audio viewing software. Additional notations may be made by any reviewing personnel at their discretion.

Any media that is unclassified will be identified by the officer/civilian's supervisor and brought to the officer/civilian's attention for correction.

VI. SUPERVISORY RESPONSIBILITIES

- A.** Supervisors will inspect the in-car video and BWCs system during their routine inspections of their officers and their officers' assigned equipment.
- B.** At least on a monthly basis, Lieutenants and Sergeants will randomly review a minimum of five (5) recordings from the in-car video camera and ten (10) recordings from the BWCs of their personnel to ensure that the equipment is operating properly and that officers are using the equipment appropriately and in accordance with policy to identify any areas in which additional training or guidance is required. Lieutenants and Sergeants, will also ensure that the officer or civilian's actions are within departmental policies, local ordinances and state and federal laws. These reviews will be documented by the Lieutenants and Sergeants within Guardian Tracking. The Lieutenants will ultimately be responsible for the review of the media files.

VII. TAPE & DIGITAL MEDIA CONTROL AND MANAGEMENT OF VIEWING SOFTWARE

- A.** All videotapes and digital media will be subject to the security restrictions and chain of evidence safeguards as outlined in standard operating procedure A060 (Evidence & Property Management). Recordings/photographs shall only be made from devices approved by the police department. In the rare occasion a personal device is needed to collect evidence, the media will, as soon as possible, be placed into evidence or attached to the incident report within the report management system (RMS). The collected data will then be immediately removed from the officer or civilian personnel's device. All digital media files will only be stored in repository systems approved by the police department or the Marietta Information Technology Department.
- B.** No photographs, video, or audio recordings will be copied for employees for personal reasons unless specifically approved by the Chief of Police. Recorded copies of an incident will only be made when requested by a

prosecutor, subpoenaed for court, necessary for departmental hearings, and for the risk analysis board.

- C. Digital photographs and video captured by the in-car system or BWCs will be maintained in Property/Evidence for a minimum period of 30 months, or until all pending criminal cases are adjudicated and all possible appeals have been exhausted, whichever is later. All digital media files that involve an arrest or any person in custody will be maintained for a minimum period of 30 months as per the Georgia Retention Schedule for Local Governments.

NOTE: If any media file contains documentation that may result in CIVIL LITIGATION involving the Marietta Police Department or its employees, the file will be maintained until litigation is resolved.

- D. All requests made under the Georgia Open Records Act shall be forwarded to the Chief of Police. Only employees authorized by the Chief of Police may disseminate the contents of department audio/video/photograph system in accordance with the Georgia Open Records Act. Personnel releasing media files from devices used by personnel of this department shall also refer to O.C.G.A. 50-18-72 (When public disclosure is not required) to include subsection 26.2. Prior to releasing any media files, proper redaction shall be made if the system allows for redaction.
- E. Access to the media viewing software shall be by individual user name and password. User names and passwords shall not be shared or transmitted to any other persons.

Chief Dan Flynn
Marietta Police Department

First Reading: 021419
Final Adoption: 032119
Distribution Date: 051619
Effective Date: 051919

Marietta Police Department

240 Lemon Street, Marietta, Georgia 30060 Telephone 770-794-5300 Fax 770-794-5301

Dan Flynn, Chief of Police



FLOCK CAMERA FAMILIARIZATION

A STATIONARY LPR SYSTEM

“Policing With A Vision”

What is the Flock Camera?

The Flock Camera is a stationary license plate reader (LPR) that is in a fixed location, usually mounted on a pole. The camera scans traffic for visible license plates and sends a recording back to the central location at Flock's headquarters. They use a cellular data service to submit these recordings. Once the data is received it is run through a known list of stolen plates and wanted persons. If the entering agency has attached the license plate of a wanted person to a GCIC entry, a notification can be generated that the car may contain a wanted occupant.

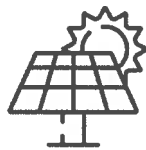
What kind of delay can I expect?

Currently, based upon my observations of the system, the delay can vary. Between the time of the camera recording the image, uploading the image, the main system checking the image, and an alert being sent out to my patrol car, a delay between as little as 5 minutes to as long as 20 minutes has been observed.



Read License Plates

Over 70% of crime occurs with a vehicle, so Flock Safety is able to capture vehicles traveling up to 55 MPH, day and night, and up to 75 ft away.



Install Everywhere

Traditional camera systems require significant infrastructure and upfront costs. Flock Safety leverages solar + battery for power, and cellular (LTE) for data communications, removing any upfront costs.



Fast Access

We store our footage in the cloud, so you can securely access the cameras from any laptop or phone.

“Policing With A Vision”

How do I get started?



An icon located on your desktop (pictured above) will open your web browser to the Flock website (<https://pd.flocksafety.com>). The website only functions under google chrome, internet explorer is not supported.

When prompted for a login...

Username: mariettaflock@mariettaga.gov

Password: Flock!Marietta

Flock Safety - Notification Tool

Please Login

mariettaflock@mariettaga.gov

.....

LOGIN

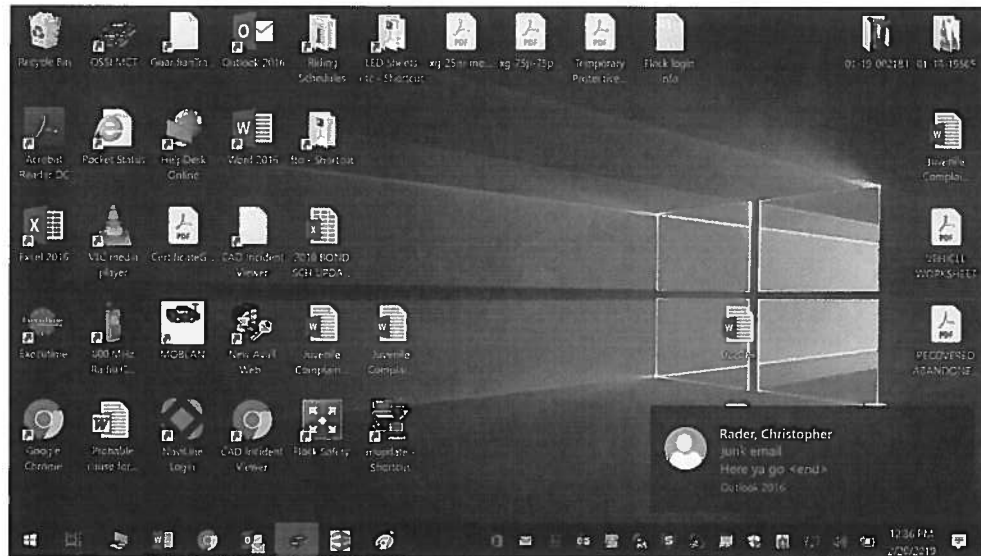
Upon logging into flock for the first time, you will be prompted to allow notifications, click Allow.

Once you have entered the username and password, chrome should ask you to save the information, click save. From here on in, unless you are switching computers, you should not have to enter a user/password again. **The system will maintain your login information and you just need to open the webpage at the start of your shift.**

“Policing With A Vision”

What does an “Alert” look like?

Currently Flock is using a windows notification similar to the one pictured below. As long as the web browser remains open, like we do for our calls for service page, you should receive an alert in the bottom right corner indicating that the Flock system has found a license plate. This alert should coincide with an audible notification as well, similar to the new mail sound.



How do I best use the system?

The Flock alert will give you information that a vehicle has passed by one of the cameras and the reason for the alert. These alerts can range from a stolen license plate, stolen vehicle, to a license plate associated with a wanted person. When an alert is received it will display a brief reason, a small photo of the license plate, and the location of the camera that took the photo. You have three buttons to interact with the tool.

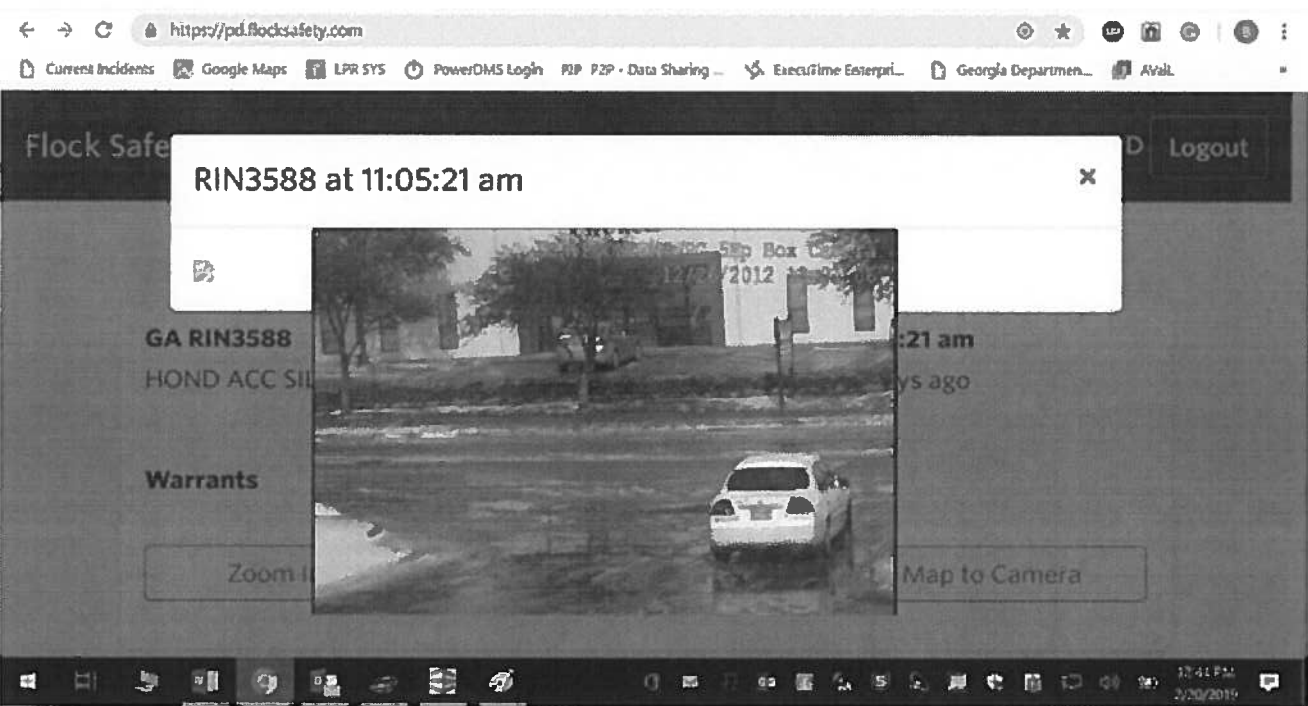
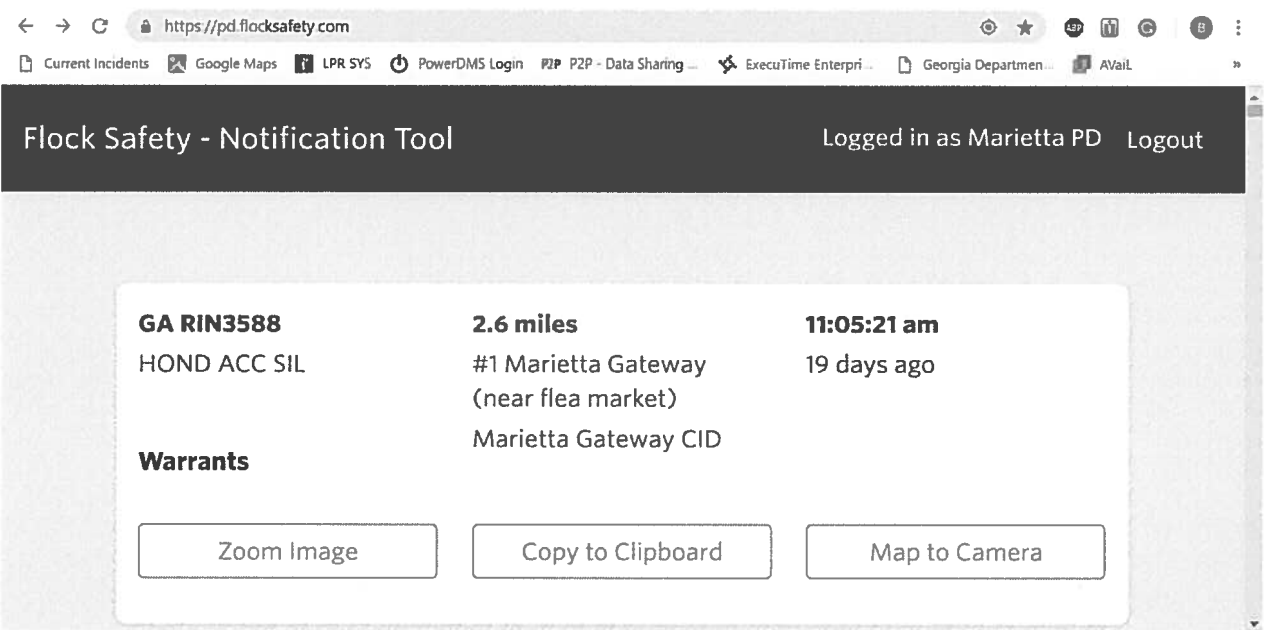
“Zoom Image” button that will allow you to compare the license plate with the vehicle that is currently displaying that plate, useful for a vehicle that is using a stolen plate that doesn’t match the vehicle being driven.

“Copy to Clipboard” will allow you to copy the license plate to easily paste back into OSSI with the keyboard shortcut CTRL + V.

“Map to Camera” will open google maps showing the location that the camera is placed.

“Policing With A Vision”

Some of the cameras are labeled “entrance” and “exit” for easy determination if that vehicle is currently entering or exiting the location the camera is located (Example: 1955 Bells Ferry Road). Other cameras might have a short description of the location, as shown below.



(Example of a “Zoomed Image”)

VERIFY ALL HIT NOTIFICATIONS THROUGH GCIC/NCIC BEFORE TAKING ACTION

“Policing With A Vision”

MEMORANDUM OF UNDERSTANDING

This Data Sharing Memorandum of Understanding (this "MOU") is entered into by and between Flock Group, Inc. with a place of business at 2588 Winslow Drive, Atlanta, GA 30305 ("Flock") and the police department or agency identified in the signature block below ("Agency") (each a "Party, and together, the "Parties").

Whereas, Agency desires to access Flock's technology platform (the "Flock Service") in order to view and search videos recorded by Flock ("Recordings") which are stored for no longer than 30 days in compliance with Georgia Records Retention policy, utilizing its software for automatic license plate detection;

Whereas, Flock desires to share such videos with Agency pursuant to the following terms and conditions.

1. **Purpose.** To allow the Agency to utilize the Flock Services for the following purpose: [to gain awareness with respect to the communities for which they serve to protect] (the "Purpose").
2. **Access Rights to Flock Services.** Subject to the terms and conditions contained in this MOU, Flock hereby grants to Agency a non-exclusive, non-transferable right to access the features and functions of the Flock Service during the Term (as defined below), solely for use by Authorized Users in accordance with the terms and conditions herein. For purposes of this MOU, "Authorized Users" will mean employees, agents, or officers of Agency accessing or using the Flock Services for the Purpose. Agency acknowledges and agrees that, as between Agency and Flock, Agency shall be responsible for all acts and omissions of Authorized Users, and any act or omission by an Authorized User which, if undertaken by Agency, would constitute a breach of this MOU, shall be deemed a breach of this MOU by Agency. Agency shall undertake reasonable efforts to make all Authorized Users aware of the provisions of this MOU as applicable to such Authorized User's use of the Flock Service, and shall cause Authorized Users to comply with such provisions.
3. **Restrictions on Use.** Agency will not, and will not permit any Authorized Users or any third party to, (i) copy or duplicate any of the Flock Service; (ii) decompile, disassemble, reverse engineer or otherwise attempt to obtain or perceive the source code from which any software component of any of the Flock Service is compiled or interpreted; (iii) modify, alter, or tamper with any of the Flock Service, or create any derivative product from any of the foregoing; (iv) interfere or attempt to interfere in any manner with the functionality or proper working of any of the Flock Service; (v) remove, obscure, or alter any notice of any intellectual property or proprietary right appearing on or contained within any of the Flock Service; or (vi) assign, sublicense, sell, resell, lease, rent or otherwise transfer or convey, or pledge as security or otherwise encumber, Agency's rights under Sections 2.
4. **Ownership.** As between the Parties, subject to the rights granted in this MOU, Flock and its licensors retain all right, title and interest in and to the Flock Service, and its components and any Recordings or data provided by Flock through the Flock Service, and Agency acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this MOU. Agency further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock's sole discretion. There are no implied rights.
5. **Financial Implications to Agency.** No financial commitment by Agency is required to access the Flock Services or Recordings.
6. **Term; Termination.**

- A. **Term.** This MOU will commence once executed by both parties and shall continue for a period of [5] years.
 - B. **Termination.** Flock may terminate this MOU for its convenience, and in its sole discretion, by providing Agency thirty (30) days prior written notice of termination. Agency may terminate this MOU for its convenience, and in its sole discretion, by providing Agency ninety (90) days prior written notice of termination. Either party may terminate this MOU upon written notice if the other party has breached a material term of this MOU and has not cured such breach within thirty (30) days of receipt of notice from the non-breaching party specifying the breach. Upon termination of this MOU, Agency will immediately cease all use of Flock Services.
7. **Indemnification.** Each Party to this MOU shall assume the responsibility and liability for the acts and omissions of its own employees, deputies, officers, or agents, in connection with the performance of their official duties under this MOU. For tort liability purposes, no participating Party shall be considered the agent of the other participating Party. Each Party to this MOU shall be liable (if at all) only for the torts of its own officers, agents, or employees that occur within the scope of their official duties. Under no circumstances shall this MOU be interpreted to create a partnership or agency relationship between the Parties.
8. **Limitation of Liability.**
- A. **Limitation on Direct Damages.** IN NO EVENT SHALL FLOCK'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO THIS MOU EXCEED \$100, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE.
 - B. **Waiver of Consequential Damages.** IN NO EVENT, UNLESS DIRECTLY CAUSED BY THE WILLFUL MISCONDUCT OF THE FLOCK GROUP, SHALL FLOCK OR ITS LICENSORS OR SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOSS OF DATA OR LOSS OF PROFITS, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF FLOCK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
9. **Confidentiality.**
- A. **Obligations.** Each of the parties agrees to maintain in confidence any non-public information of the other party, whether written or otherwise, disclosed by the other party in the course of performance of this MOU that a party knows or reasonably should know is considered confidential by the disclosing party ("Confidential Information"). The parties hereby agree that Confidential Information includes the terms and conditions of this MOU, and any discussions related thereto as well as the Flock Services. The receiving party shall not disclose, use, transmit, inform or make available to any entity, person or body any of the Confidential Information, except as a necessary part of performing its obligations hereunder, and shall take all such actions as are reasonably necessary and appropriate to preserve and protect the Confidential Information and the parties' respective rights therein, at all times exercising at least a reasonable level of care. Each party agrees to restrict access to the Confidential Information of the other party to those employees or agents who require access in order to perform hereunder, and, except as otherwise provided, neither party shall make

Confidential Information available to any other person or entity without the prior written consent of the other party.

B. **Exclusions.** Confidential Information shall not include any information that is (i) already known to the receiving party at the time of the disclosure; (ii) publicly known at the time of the disclosure or becomes publicly known through no wrongful act or failure of the receiving party; (iii) subsequently disclosed to the receiving party on a non-confidential basis by a third party not having a confidential relationship with the other party hereto that rightfully acquired such information; or (iv) communicated to a third party by the receiving party with the express written consent of the other party hereto. A disclosure of Confidential Information that is legally compelled to be disclosed pursuant to a subpoena, summons, order or other judicial or governmental process shall not be considered a breach of this MOU; provided the receiving party provides prompt notice of any such subpoena, order, or the like to the other party so that such party will have the opportunity to obtain a protective order or otherwise oppose the disclosure.

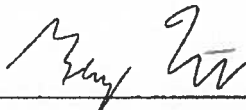
C. **Open Records.** Flock understands that Marietta, as a Public Entity, is subject to the Georgia Open Records Act and Marietta may be required to provide information received from Flock if requested. In the event such a request occurs, Marietta will provide advance notice to Flock.

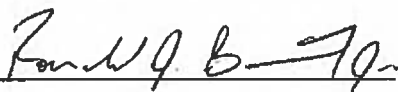
10. **Miscellaneous.** All notices, requests, demands, or other communications required or permitted to be given hereunder must be in writing and must be addressed to the parties at their respective addresses set forth below and shall be deemed to have been duly given when (a) delivered in person; (b) sent by facsimile transmission To the facsimile number below and indicating receipt at the facsimile number where sent; (c) one (1) business day after being deposited with a reputable overnight air courier service; or (d) three (3) business days after being deposited with the United States Postal Service, for delivery by certified or registered mail, postage pre-paid and return receipt requested. This MOU shall be governed by the laws of the state of [Georgia], excluding its conflict of laws rules. The parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this MOU.

IN WITNESS WHEREOF, Flock and the Agency have caused this MOU to be signed on the date set forth below and be effective on the last date specified below.

Flock Group, Inc.:

Agency: CITY OF MARIETTA, GA

By: 

By: 

Name: **Bailey Quintrell**

Name: RONALD J. BARRETT JR.

Title: **Head of Public Safety**

Title: DIRECTOR OF INFORMATION TECHNOLOGY

