ORDER NO. 29

OFFICIAL ORDER
MICHIGAN STATE POLICE

SUBJECT: Fingerprints and Criminal History Record Information

TO: Department Members

This Order establishes department policy and member responsibilities for the following:

29.1 FINGERPRINTS, CRIMINAL HISTORY INFORMATION, AND CRIMINAL RECORDS

This section defines the duties of members as they relate to fingerprinting persons and processing fingerprints. The section also defines the responsibilities of members as they relate to criminal history information and changes to criminal record information maintained by the Criminal Justice Information Center (CJIC).

29.1.1. ARREST FINGERPRINTING OF ADULT AND JUVENILE OFFENDERS

A. MCL 28.241 designates the department as the state central repository for collection and filing of criminal and juvenile history records. The Bureau of Criminal Identification and Records Act specifies that local law enforcement agencies shall fingerprint any adult or juvenile arrested for a felony, high court misdemeanor, or ordinance that directly corresponds to a state statute.

(1) Arrest fingerprints shall be taken using a Live Scan machine and submitted electronically. Palm prints must be taken when the electronic capability is available.

(2) The work unit commander shall coordinate with local criminal justice officials to ensure that arrest and charging information is properly reported to the CJIC.

B. Individuals arrested for felonies, misdemeanors punishable by imprisonment that exceeds 92 days, local ordinance violations, and violations of Personal Protection Orders shall be fingerprinted. Individuals who refuse to allow or resist the taking of their fingerprints or palm prints may be charged with a misdemeanor according to MCL 28.243a.

C. Per MCL 28.243(5) enforcement members may fingerprint individuals arrested for a misdemeanor punishable by imprisonment for 92 days or less as provided in MCL 28.243(5); per MCL 28.243(13) it is not permitted to forward fingerprints of persons

convicted under the Michigan vehicle code (MCL 257.1 to 257.923) unless the first or subsequent offense of the conviction is punishable for more than 92 days.

D. Individuals missing all ten fingers or with very poor fingerprints, may not have classifiable fingerprints available. Criminal History Records that do not have identifiable prints are indicated on the identification segment of the record stating "AFIS PRINTS AVAILABLE: NO."

E. Federal fingerprints which are unclassifiable will be rejected back to the Live Scan site where the prints were collected.

Work unit commanders shall determine whether the subject is still available for fingerprinting. If the subject is available, he or she shall be re-fingerprinted.

F. Palm Printing

(1) Department work units shall palm print all subjects they arrest when capture capability is available via Live Scan.

(2) A Law Enforcement Information Network (LEIN) inquiry of the criminal history record will identify the existence of palm prints in Automated Fingerprint Identification System (AFIS) at the Biometrics and Identification Division (BID).

(3) Palm print files are accessible on request by e-mail to FPLOOKUP@MICHIGAN.GOV, written correspondence, facsimile, or telephone.

29.1.2. MODIFICATION AND DELETION OF ARREST PRINTS

A. Members shall immediately notify the CJIC, via LEIN, to delete fingerprints related to a subject if the subject is not charged for prosecution or petitioned into probate court as a juvenile offender.

The notification for modification of arrest prints is completed by using the forms tab in LEIN. Select "Criminal History", then "Modify Arrest to REL" (Release). When the form appears, enter the Transaction Control Number (TCN), Agency Case Number (OCA), Arresting Agency ORI, and confirm the Arrest Disposition Code is REL, then transmit. The transaction and the incident are closed and retained as a non-public record, until such time that the CJIC deletes the arrest incident.

B. MCL 28.243(11) requires reporting of final disposition from the clerk of the court. For cases when the finding was "not guilty," or the juvenile adjudication was dropped, this statute provides for the destruction of the fingerprint image if the subject was not arraigned for any of the offenses specified in MCL 28.243(14) and has no prior conviction other than traffic on file.

(1) The CJIC shall notify the Federal Bureau of Investigation (FBI) to remove the arrest image at the same time.

(2) The department work unit which provided the arrest information will not be notified.

C. Unless the return or destruction of fingerprints is specifically required by MCL 28.243, the CJIC and the BID shall only destroy the fingerprints by order of the court of jurisdiction.

(1) A copy of the court order is submitted to the CJIC by the court of jurisdiction.

(2) The CJIC shall request the BID to remove the fingerprints from AFIS.

(3) The department work unit which provided the arrest information will not be notified by the CJIC of the destruction of the images.

D. When an original conviction is dismissed through appeal and a new trial, the court of final jurisdiction will provide the modified disposition to the CJIC, which shall request the BID to remove the fingerprints from the AFIS.

29.1.3. MISDEMEANOR ARRESTS

A. MCL 28.243(1) specifies that when a person is arrested for a misdemeanor punishable by more than 92 days or a $1,000 fine, including violations of the Michigan Vehicle Code, the person's fingerprints shall be taken and submitted within 72 hours. The arresting worksite shall submit fingerprints electronically through Live Scan in order to create a criminal history record. The department work unit should notify the court of jurisdiction that this information has been submitted.

B. The following traffic misdemeanors must be submitted electronically via Live Scan, regardless of the maximum sentence. This same requirement applies to any local ordinances that correspond to these state statutes.

PACC Charge Code	MCL No.	Description
257.6251- A	257.625(1)	Operating While Intoxicated (OWI)
257.6258	257.625(8)	Operating With Any Presence of Drugs (OWPD)
257.6253- A	257.625(3)	Operating Impaired
257.9041B	257.904(1)(b)	Operating license suspended, revoked, denied &/or allowing suspended person to operate
257.9041- A	257.904(1)(a)	Operating--suspended for failure to answer citation

29.1.4. COURT ORDERED FINGERPRINTING

A. MCL 764.29 specifies that on arraignment of a subject for a felony or misdemeanor punishable by more than 92 days, the court file is examined to determine if the fingerprints have been taken If a court determines that fingerprints were not taken and submitted as required upon arrest, the court shall order that the fingerprints be taken and submitted through Live Scan.

B. If the arrest record was not created on the criminal history system, the magistrate shall order the subject to submit to fingerprinting by the police agency who obtained the warrant or by the sheriff.

(1) When a person is ordered to a department work unit for fingerprinting, the unit shall verify that the arrest has not already been created on the criminal history. Run a criminal history record inquiry via the LEIN using the criminal tracking

number or subject name from the order. Examine the criminal history Record to determine if the criminal tracking number is already on file.

(2) If it is determined that fingerprints have already been submitted for the incident, a copy of the documentation shall be attached to the order and returned to the court of jurisdiction.

(3) If there is no evidence the subject has been fingerprinted for the incident, the subject's fingerprints shall be collected and submitted via Live Scan.

29.1.5. FUGITIVE ARRESTS

A. Only warrant-holding agencies should submit arrest fingerprints.

B. Subjects held for out-of-state extradition may be submitted as an ID only (Retention = N).

C. The Michigan Department of Corrections (MDOC) is the warrant holding agency for subjects who are apprehended and charged for prison escape. The MDOC will be carried as the arresting department.

D. When using Live Scan to process a subject arrested on a failure to appear bench warrant, the subject's criminal history record shall be checked to determine whether they had been previously fingerprinted for the incident.

(1) If the arrested subject had not been previously fingerprinted, their fingerprints shall be submitted as a record build (Retention = Y).

(2) If the arrested subject had been previously fingerprinted, their fingerprints shall either not be submitted or submitted as an ID Only (Retention = N).

29.1.6. NONPUBLIC OR SEALED RECORDS

A. Courts of jurisdiction shall report dispositions to the CJIC to be entered in the criminal history records as sealed for the following Michigan Compiled Laws:

(1) 333.7411 - Controlled Substance Act

(2) 600.1076 – Drug Treatment Court

(3) 600.1098 – Mental Health Court

(4) 600.1206 & 600.1209 – Veterans Treatment Court

(5) 712A.2f – Juvenile Consent Calendar

(6) 750.350a – Parental Kidnapping

(7) 750.430 – Practicing Under the Influence

(8) 750.451c – Human Trafficking Victim

(9) 762.11 to 762.15 – Holmes Youthful Trainee Act

(10) 769.4a – Spouse Abuse

B. On receipt of the sentence disposition, the CJIC shall enter the disposition and control dissemination to criminal justice agencies and the subject of record.

C. The CJIC does not notify the originating work unit when the record is sealed from public access.

D. Under MCL 769.16a(8), for cases that end without a conviction, the CJIC shall remove all information indicating the person was convicted of the offense from databases that are available to the public.

29.1.7. APPLICANT FINGERPRINTING

A. Department work units may fingerprint new employees and submit the fingerprints via Live Scan for processing. For all other criminal justice employment fingerprint requests, the subject should be directed back to the hiring law enforcement agency.

B. Department work units may fingerprint for any of the following fingerprint reasons using RI-008 print cards or direct the subject to a local police agency. These requests are the only fingerprints accepted using RI-008 print cards:

(1) Adoption

(2) Conviction Set-Aside Application (adult and juvenile)

C. Department work units which are the arresting agency will receive a copy of the court order directly from the court. The work unit files shall be modified to reflect the disposition and shall control dissemination.

D. MCL 780.623 and 712A.18e provide that any person other than the applicant who divulges, uses, or publishes information concerning the set aside conviction or adjudication, except as provided in the statute, is guilty of a misdemeanor

(1) Fingerprint Registration

(2) Housing Commission

(3) Name Change

(4) Personal Record Review

(5) Record Challenge

(6) Visa/Immigration Application

E. When fingerprinting for any of the reasons in Section 29.1.7.B, members shall:

(1) Verify the subject's personal identification and compare the signature on the applicant fingerprint card, RI-008, to the presented identification.

(2) After fingerprinting and completely filling out the fingerprint card, the fingerprint card shall be returned to the subject for submission with their application.

(3) The fingerprinting work unit shall not appear as the contributor on the card.

F. Applicant fingerprints shall be retained in the AFIS database unless prohibited by statute.

G. Applicant fingerprint cards, RI-008, can be obtained from the Resource Management Unit.

H. Department work units shall not utilize RI-008 fingerprint cards or Live Scan devices to print applicants for any reasons not listed in Section 29.1.7.B. Instead, the citizen should be directed to an agency authorized to collect those applicant fingerprints.

29.1.8. LATENT LIFT COMPARISON

A. Fingerprinting needed for laboratory latent print comparison elimination shall be done on the applicant fingerprint card, RI-008.

B. Forensic Science Division crime laboratories shall be responsible for all department latent print comparisons.

29.1.9. SETTING ASIDE CONVICTIONS

A. Department work units which are the arresting agency will receive a copy of the court order directly from the court. The work unit files shall be modified to reflect the disposition and shall control dissemination.

B. MCL 780.623 and 712A.18e provide that any person other than the applicant who divulges, uses, or publishes information concerning the set aside conviction or adjudication, except as provided in the statute, is guilty of a misdemeanor.

29.1.10. DISSEMINATION

A. Secondary dissemination of Michigan criminal history record information by a department work unit other than the CJIC is limited by the Michigan CJIS Administrative Rules, LEIN policy, National Crime Information Center (NCIC) policy, the FBI CJIS Security Policy, the Michigan Addendum to the FBI CJIS Security Policy, and Executive Order 1990-10.

B. Requests for criminal history record information other than those authorized by the references listed above, including personal records checks, shall be directed to the CJIC.

29.1.11. PROCESSING CHALLENGES TO PUBLIC RECORDS

A. Responsibilities of Worksite Commanders

(1) An individual who is the subject of a criminal history record which he or she believes either does not belong to them or has inaccurate information on it has the right to seek correction of the record.

a. Individuals who believe the criminal history record does not belong to them shall be fingerprinted on an RI-008, Applicant Fingerprint Card. The member shall direct the individual to mail the fingerprint card with a copy of the record in question to the CJIC, indicating the need for a record challenge.

b. Individuals who have an inaccurate criminal history record shall be directed to contact the contributing agency to provide any documentation to CJIC.

B. Responsibilities of the CJIC

(1) The CJIC shall conduct an investigation into the request by:

a. Reviewing the contested record.

b. Reviewing evidence of error presented by the requestor.

c. Requesting field assistance to verify inconsistencies.

(2) The CJIC shall act on the request within 30 business days of receipt of the request.

(3) Acting on the evidence found, the CJIC shall render a decision and advise the requestor in writing of the decision.

a. If the requestor's claim is sustained, the disputed record shall be modified by the CJIC.

b. If the requestor's claim is denied, he or she shall be informed.

C. Appeal Process

(1) A person whose request to have a department record modified has been denied may appeal this decision to the CJIC.

(2) If the CJIC affirms the decision, the requestor shall be notified in writing. The requestor shall also be informed that he or she may pursue the matter further by commencing court action.

29.2 CRIMINAL HISTORY RECORD INFORMATION (CHRI)

CHRI maintained by the department is subject to federal regulations and state procedures. This section details responsibilities of the department and its members concerning collection, storage, and dissemination of these records.

29.2.1. DEFINITIONS

A. 28 CFR Part 20

28 CFR Part 20 refers to the federal regulations requiring the collection, storage, and dissemination of CHRI in a manner to ensure the accuracy, completeness, currency, integrity and security of such information and to protect individual privacy.

B. Criminal Justice Agency

"Criminal justice agency" means courts; and a government agency or any subunit thereof that performs the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part (over 50%) of its annual budget to the administration of criminal justice. State and Federal Inspector General Offices are included.

C. Administration of Criminal Justice

The "administration of criminal justice" means performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information.

D. CHRI

CHRI means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

E. National Crime Information Center/Interstate Identification Index (NCIC/III)

NCIC/III is the national index of computerized criminal histories available via NCIC or the International Justice and Public Safety Network (Nlets), identified and indexed from data received on FBI fingerprint submissions.

F. Law Enforcement Information Network (LEIN)

"LEIN" means the Michigan Law Enforcement Information Network.

29.2.2. AGENCIES SUBJECT TO 28 CFR Part 20

The Michigan State Police is subject to 28 CFR Part 20 along with any recipient of CHRI maintained by the department.

29.2.3. ACCOUNTABILITY FOR CHRI REQUESTS

Department work units having direct access to the Michigan/CHRI, NCIC and III shall follow LEIN rules and procedures concerning access to these files.

A. CHRI files shall be accessed for official business only.

B. Requests for CHRI from a device with direct access to LEIN shall contain the purpose of the query, the name of the terminal operator, the name of the person requesting the inquiry and the identity of their agency, and any other data pertinent to the dissemination or use of the information.

C. LEIN device requests for CHRI shall automatically be logged by the CJIC.

D. District and division commanders, the Field Support Section of the CJIC, and state and federal auditors may use the computerized log file for auditing purposes.

29.2.4. CHRI DISSEMINATION POLICY

A. The CHRI files maintained by the department are restricted on a right-to-know basis. Criminal justice agencies may receive CHRI for the purpose of the administration of criminal justice and criminal justice employment.

B. Except as allowed in paragraph C below, members of the department shall not obtain CHRI for, nor directly or indirectly supply CHRI to, citizens, private guard or detective agencies, insurance companies, National Guard, U.S. Military recruiters, private attorneys, non-criminal justice agencies, or others who do not have a legal right to such data.

C. CHRI may be released by the CJIC to other than criminal justice agencies if so determined by the CJIC director in accordance with the CJIS Administrative Rules to be within legal and policy restraints.

D. Requests for CHRI which cite the Michigan Freedom of Information (FOI) Act shall be processed according to Official Order 20 and shall be disseminated by the Records Resource Section (RRS).

E. Certain State of Michigan departments, or subunits of those departments, are eligible for Michigan CHRI information authorized by Executive Order 1990-10. Refer to the LEIN operation manual for correct purpose code to be used in the inquiry.

F. Out-of-State Requests.

Requests received from an out-of-state source shall be referred to the CJIC for review of authority and response. Out-of-state requests for CHRI shall not be answered by posts or units.

G. Member Responsibility

Members having access to CHRI are personally responsible and individually liable for misuse by themselves or by an unauthorized person to whom they furnish information. Any agency or individual violating Title 28 policies for use and dissemination of CHRI shall be subject to a fine not to exceed $10,000. Members are also subject to department discipline according to Official Order No. 1.

29.2.5. RELEASE TO NEWS MEDIA

All requests for CHRI by the news media, shall be forwarded to the RRS for processing and shall be released according to the Michigan CJIS Administrative Rules and Title 28.

29.3 MOBILE FINGERPRINT IDENTIFICATION (MOBILE ID) TECHNOLOGY

This section establishes procedures for the acceptable use of Mobile Fingerprint Identification (Mobile ID) technology. All technology associated with Mobile ID, including all related hardware and software support, is bound by the FBI Criminal Justice Information Services (CJIS) Security Policy, particularly Policy Area 13, and the Michigan CJIS Security Addendum.

29.3.1. DEFINITIONS

A. “Authorized User (User)” is an individual employed as a law enforcement officer, or a civilian employed by a criminal justice agency, whose agency is approved by the department to utilize Mobile ID.

B. “Criminal Justice Information (CJI)” is all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

C. “Mobile Fingerprint Identification (Mobile ID)” is the process by which a fingerprint scanner is used in a mobile environment to attempt to identify an individual whose identity is questioned. The scanned fingerprint images are then compared to fingerprints stored in the Michigan Automated Fingerprint Identification System (AFIS) and the FBI Repository of Individuals of Special Concern (RISC) databases.

D. “Mobile Fingerprint Scanner (Scanner)” is a fingerprint capture device used to scan fingerprints directly from the finger and electronically transmit the captured fingerprint images to Michigan AFIS and FBI RISC databases.

E. "Personally Identifiable Information (PII)" is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

29.3.2. AUTHORIZED USE

Mobile ID shall only be used during the course of a User's lawful duties and one of the following circumstances exists:

A. With Consent of an Individual 17 Years of Age or Older

(1) Mobile ID may be used with consent of an individual 17 years of age or older during the course of a User's lawful duties. The individual may limit or withdraw consent at any time. If consent is withdrawn and use of Mobile ID is solely based upon consent, use of Mobile ID is not authorized and its use must stop immediately.

B. With Consent of an Individual Under 17 Years of Age and Parent or Guardian

(1) The Child Identification and Protection Act, 1985 PA 176, MCL 722.771-772.775, prohibits fingerprinting children, persons under 17 years of age, except under the limited circumstances prescribed in MCL 722.774.

(2) Mobile ID may be used with written consent of the child and their parent or guardian during the course of a User's lawful duties. The child and their parent or guardian may limit or withdraw consent at any time. If consent is withdrawn by either the child or their parent or guardian and use of Mobile ID is solely based upon consent, use of Mobile ID is not authorized and its use must stop immediately.

(3) Given that Mobile ID is used when the identity of an individual is questioned, a User may be unable to accurately determine an individual's age. In the event that Mobile ID is used to identify an individual who the User reasonably believed was 17 years of age or older, but subsequently determined to be under 17 years of age, the User must document all information upon which he or she reasonably relied in determining the individual was 17 years of age or older.

C. Without Consent of an Individual

(1) Mobile ID may be used without consent of an individual of any age if one of the following circumstances exists:

a. The User has probable cause to believe the individual has committed a crime for which fingerprinting is allowable under MCL 28.243.

b. The individual is unable to provide reliable identification due to physical incapacitation or defect, mental incapacitation or defect, or death, and immediate identification is needed to assist the User in performance of their lawful duties. The User shall not use the Scanner to identify a person for purposes of certification of death. Official requests for certification of identity should be submitted to the MSP Ten-Print Analysis and Identification Unit (fingerprint technicians) at MSP Headquarters, or the Latent Fingerprint Unit at one of the MSP laboratories.

c. Pursuant to a valid court order.

29.3.3. IDENTIFICATION PROCESS

After fingerprint images are captured by the Scanner, the images are electronically transmitted to Michigan AFIS and FBI RISC databases where a non-assisted fingerprint search is performed. The captured fingerprint images are not retained on the Scanner. After completion of the non-assisted fingerprint search, one of the following responses is returned to the User via an electronic device linked to the Scanner:

A. "Hit" – This response means an identification match was made. An individual's name, date of birth, sex, race, state identification number, and mug shot photo are returned to the User.

B. "No Record was Returned" – This response means no identification match was made.

C. "Unable to Determine" – This response means possible candidates were found, but the scoring of such identifying fingerprints are below a defined criteria threshold used to confirm a positive "Hit" without human intervention. Up to five possible individuals' names, dates of birth, sex, race, state identification numbers and mug shot photos may be returned to the User.

Individual identifications as a result of Mobile ID are limited to individuals maintained in the Michigan AFIS and FBI RISC databases and does not preclude a record from existing in other biometric or name-based repositories.

29.3.4. DISCLOSURE AND USE OF INFORMATION

A. The information contained in a Mobile ID response may contain PII or CJI which may only be transmitted, accessed, used, disseminated, and disposed of in accordance with state and federal laws, rules, policies, and regulations; including, but not limited to the most recent FBI Criminal Justice Information Services (CJIS) Security Policy, the Michigan Addendum to the FBI CJIS Security Policy, the CJIS Policy Council Act, 1974 PA 163, MCL 28.211-28.216, and the most current CJIS Administrative Rules.

B. Improper access, use or dissemination of PII or CJI obtained from use of Mobile ID may result in criminal penalties and/or administrative sanctions.

29.3.5. DOCUMENTATION

All Mobile ID use, including use of Mobile ID to assist another law enforcement agency, shall be documented by the User in an original incident report, if an original incident report regarding the incident is being completed, or as an entry on the enforcement member's daily. At a minimum, the documentation shall include the date, time, location, and justification for utilizing Mobile ID.

29.3.6. AUDITING AND PENALTIES FOR MISUSE

All Mobile ID use is subject to audit by the MSP. All audit findings and administrative sanctions imposed are at the sole discretion of the MSP. Penalties that may be imposed include, but are not limited to, termination of a User's access to Mobile ID, termination of a Scanner's access to Mobile ID, and termination of agency-wide access to Mobile ID.

29.4 STATEWIDE NETWORK OF AGENCY PHOTOS (SNAP)

This section establishes procedures for acceptable use of the images, information, and tools within the Statewide Network of Agency Photos (SNAP) application.

29.4.1. DEFINITIONS

A. "Biometric data" is data derived from one or more intrinsic physical or behavioral traits of humans, to include fingerprints, palm prints, iris scans, and facial recognition data.

B. "Facial recognition (FR)" is the automated searching of a facial image in a biometric database (one-to-many), typically resulting in a group of facial images ranked by computer-evaluated similarity.

C. "Highly Restricted Personal Information" is an individual's photograph or image, social security number, digitized signature, medical and disability information.

D. "Mobile Facial Recognition (Mobile FR)" is the process of conducting an automated FR search in a mobile environment.

E. "Statewide Network of Agency Photos (SNAP)" is a computer application managed by the SNAP Unit, deployed through the Michigan Criminal Justice Information Network (MiCJIN) Portal, which serves as an investigative tool and a central repository of images from local, state, and federal agencies.

F. "User" is an individual who is authorized to access the SNAP application and whose agency is approved by the Michigan Department of State Police (MSP) to utilize the SNAP.

29.4.2. DISCLOSURE AND USE OF INFORMATION

A. All technology associated with the SNAP, including all related hardware and software support, is bound by the FBI CJIS Security Policy, particularly Policy Area 13, and the Michigan Addendum to the FBI CJIS Security Policy.

B. The information within the SNAP databases is considered highly restricted information which may only be transmitted, accessed, used, disseminated, and disposed of in accordance with state and federal laws, rules, policies, and regulations; including, but not limited to, the most recent FBI CJIS Security Policy, the Michigan Addendum to the FBI CJIS Security Policy, the CJIS Policy Council Act (1974 PA 163), MCL 28.211-28.216, and the most current CJIS Administrative Rules.

C. Improper access, use, or dissemination of highly restricted information obtained from the use of the SNAP may result in criminal penalties and/or administrative sanctions. Criminal violations include, but are not limited to, those found in MCL 28.214 and MCL 257.903.

29.4.3. MICHIGAN DEPARTMENT OF STATE (MDOS) IMAGES

The SOS database contains a copy of images captured by the MDOS. MDOS images are considered highly restricted personal information that may be used by a federal, state, or local governmental agency for a law enforcement purpose authorized by law.

A. When possible, other photographs (e.g., criminal mug shots, personal photographs) should be used rather than MDOS images.

B. When releasing MDOS images to the public for law enforcement purposes (e.g., wanted posters, flyers), all information identifying the image as an MDOS image shall be removed.

C. MDOS images shall not be used for candidates other than the primary suspect in a photo lineup. An MDOS image of the primary suspect may be used as part of a photo lineup. Photo lineups shall not include individuals age 16 or under at the time of image capture.

MCL 712A.32 provides the court with the power to order a juvenile to appear for identification by another person.

29.4.4. CRIMINAL MUG SHOTS AND SCAR, MARK, AND TATTOO (SMT) IMAGES

A. Policy regarding the public release of criminal mug shot images may vary by agency. Prior to releasing an image to the public, approval shall be received from the originating agency.

B. Prior to releasing an image to the public, the User shall ensure that the individual's criminal history reflects a corresponding record associated with the image and the image is not exempt from public release.

C. Criminal mug shot images may be used as the primary suspect and all other candidates in a photo lineup. Photo lineups shall not include individuals age 16 or under at the time of image capture. MCL 712A.32 provides the court with the power to order a juvenile to appear for identification by another person.

29.4.5. FACIAL RECOGNITION (FR)

A. FR is not a form of positive identification and results shall be considered an investigative lead only. If an Investigative Lead Report is generated based on an FR search, it does not serve as probably cause for arrest.

B. MSP members shall only use department-issued devices for Mobile FR. Local agencies are responsible for establishing their own policy regarding the use of personal devices for Mobile FR in accordance with the FBI CJIS Security Policy. Additionally, local agencies must sign an agreement with the MSP prior to access and use of the Mobile FR application.

C. Mobile FR shall only be used during the course of a User's lawful duties and one of the following circumstances exists:

(1) Mobile FR may be used with consent of an individual:

a. The individual may withdraw consent at any time. If consent is withdrawn, and the use of Mobile FR is solely based upon consent, use of Mobile FR is not authorized and its use must stop immediately.

(2) Mobile FR may be used without consent of an individual if one of the following circumstances exists:

a. The User has probable cause to believe the individual has committed a crime for which the collection of biometric data is allowable under MCL 28.243.

b. The individual is unable to provide reliable identification due to physical incapacitation or defect, mental incapacitation or defect, or death, and immediate identification is needed to assist the User in performance of their lawful duties.

c. Pursuant to a valid court order.

D. Users shall indicate the purpose for utilizing Mobile FR.

E. Select Users may be configured to receive MDOS images in Mobile FR results. Users with access to MDOS images in Mobile FR results shall adhere to the following:

(1) Pre-existing images, including, but not limited to, social media photos and surveillance stills, shall not be submitted through Mobile FR. Failure to comply will result in the User's access to MDOS images in Mobile FR results being terminated.

(2) Users agree to complete additional training and testing as provided by the MSP Digital Analysis and Identification Section in order to maintain access to MDOS images in the Mobile FR results. This will require written acknowledgement of understanding and agreement to adhere to the SNAP Acceptable Use Policy.

29.4.6. WATCHLIST

A. Images uploaded into the WATCHLIST must be legally obtained and the User shall have a legal right to use the image for law enforcement purposes.

B. Once the individual has been located, the User shall contact the SNAP Unit to request removal of the image from the WATCHLIST.

29.4.7. AUDITING AND PENALTIES FOR MISUSE

A. All FR use is subject to audit by the MSP SNAP Unit. In the event of an audit, the User will be required to provide appropriate justification for the use of FR. Appropriate justification may include a case/complaint number and file class/crime type, if available, or a situation description and purpose for the search. For searches conducted on behalf of another individual, the name and rank/job title of other individual requesting the search shall also be included.

B. All audit findings and administrative sanctions imposed are at the sole discretion of the MSP. Penalties that may be imposed include, but are not limited to, termination of a User's access to SNAP and termination of agency-wide access to SNAP.

29.5 REVISION RESPONSIBILITY

Responsibility for continuous review and revision of this Order lies with the Field Support Bureau (CJIC and BID), in cooperation with Executive Operations.

DIRECTOR