



SUBJECT: Fingerprints and Criminal History Record Information

TO: Members of the Department

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

<u>Section 29.1</u>	FINGERPRINTS, CRIMINAL HISTORY INFORMATION, AND CRIMINAL RECORDS	2
<u>29.1.1.</u>	Arrest Fingerprinting of Adult and Juvenile Offenders	2
<u>29.1.2.</u>	Deleting Arrest Prints	3
<u>29.1.3.</u>	Misdemeanor Arrests	4
<u>29.1.4.</u>	Court Ordered Fingerprinting	5
<u>29.1.5.</u>	Fugitive Arrests	5
<u>29.1.6.</u>	Nonpublic or Sealed Records	5
<u>29.1.7.</u>	Applicant Fingerprinting	6
<u>29.1.8.</u>	Latent Lift Comparison	7
<u>29.1.9.</u>	Setting Aside Convictions	7
<u>29.1.10.</u>	Dissemination	7
<u>29.1.11.</u>	Processing Challenges to Public Records	8
<u>Section 29.2</u>	CRIMINAL HISTORY RECORD INFORMATION	9
<u>29.2.1.</u>	Definitions	9
<u>29.2.2.</u>	Agencies Subject to Title 28 Regulations	10
<u>29.2.3.</u>	Accountability for CHRI Requests	10
<u>29.2.4.</u>	CHRI Dissemination Policy	10
<u>29.2.5.</u>	Release to News Media	11
<u>Section 29.3</u>	MOBILE FINGERPRINT IDENTIFICATION (MOBILE ID) TECHNOLOGY	11
<u>29.3.1.</u>	Definitions	11
<u>29.3.2.</u>	Authorized Use	12

29.3.3.	Identification Process	13
29.3.4.	Disclosure and Use of Information	13
29.3.5.	Documentation	13
29.3.6.	Auditing and Penalties for Misuse	13
Section 29.4	STATEWIDE NETWORK OF AGENCY PHOTOS (SNAP)	14
29.4.1.	Definitions	14
29.4.2.	Disclosure and Use of Information	14
29.4.3.	Michigan Department of State (MDOS) Images	15
29.4.4.	Criminal Mug Shots and Scar, Mark, and Tattoo (SMT) Images	15
29.4.5.	Facial Recognition (FR)	15
29.4.6.	WATCHLIST	16
29.4.7.	Auditing and Penalties for Misuse	16
Section 29.5	REVISION RESPONSIBILITY	16

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 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. DELETING ARREST PRINTS

- A. Department members shall immediately notify the CJIC to delete fingerprints related to a subject if the subject is not charged for prosecution or petitioned into probate court as a juvenile offender.

Notification for deletion of arrest prints should be done via the forms tab in the TALON (LEIN Application), then select the criminal history option. Select modify arrest to REL (Release). When the form appears, enter the Transaction Control Number (TCN), Originating Case Agency (OCA), and arresting agency ORI, then transmit the transaction and the incident is closed.

- B. [MCL 28.243](#)(9) 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 (12) and has no prior conviction other than traffic on file.
 - (1) The CJIC shall notify the Federal Bureau of Investigation 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, the person's fingerprints shall be taken and submitted to the BID within 72 hours.
- (1) When reporting a misdemeanor arrest to the CJIC, the arresting agency shall submit the arrest electronically via Live Scan. The arresting agency should forward information verifying that a criminal history record build occurred to the court of jurisdiction.
 - (2) The court of jurisdiction shall submit the final disposition to the CJIC. The court must include the TCN/OCA or the disposition.
 - (3) If the misdemeanor arrest results in placement of the subject on deferred judgment probation under the provisions of [MCL 333.7411](#) – Controlled Substance; [MCL 600.1076](#) – Drug Treatment Court; [MCL 762.11 to 762.15](#) – Holmes Youthful Trainee Act; [MCL 769.4a](#) – Spouse Abuse; [MCL 750.350a](#) – Parental Kidnapping; [MCL 750.430](#) – Practicing Under the Influence; and [MCL 600.1209](#) – Veterans Treatment Court; the court of jurisdiction must submit the disposition immediately at time of probation.
- B. Department members shall fingerprint at arrest all persons arrested for violations of the Michigan Vehicle Code for which the possible punishment exceeds 92 days or a \$1,000 fine.
- C. The following traffic misdemeanors must be reported to the CJIC, 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. [MCL 769.16a\(5\)](#) specifies that if the offense is one that requires fingerprints and fingerprints were not taken at the time of sentencing, the court shall order the fingerprints of the convicted be taken and forwarded to the MSP.
- 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 at the CJIC.
 - (2) If it is determined that fingerprints have already been submitted to the BID 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 as a record build.

29.1.5. FUGITIVE ARRESTS

- A. Only warrant-holding agencies should submit arrest fingerprints to the BID.
- B. Subjects held for out-of-state extradition are not reportable to the CJIC.
- C. The Michigan Department of Corrections is the warrant holding agency for subjects who are apprehended and charged for prison escape. The Michigan Department of Corrections 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) [436.1703](#) – Minor in Possession
 - (3) [600.1076](#) – Drug Treatment Court

- (4) [600.1098](#) – Mental Health Court
 - (5) [600.1206](#) & [600.1209](#) – Veterans Treatment Court
 - (6) [712A.2f](#) – Juvenile Consent Calendar
 - (7) [750.350a](#) – Parental Kidnapping
 - (8) [750.430](#) – Practicing Under the Influence
 - (9) [750.451c](#) – Human Trafficking Victim
 - (10) [762.11](#) to 762.15 – Holmes Youthful Trainee Act
 - (11) [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 MSP 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 to the CJIC and the BID 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)
 - (3) Fingerprint Registration
 - (4) Housing Commission
 - (5) Name Change
 - (6) Personal Record Review
 - (7) Record Challenge
 - (8) Visa/Immigration Application
- C. When fingerprinting for any of the reasons in Section 29.1.7.B, department 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.
- D. Applicant fingerprints shall be retained by the BID in the AFIS database unless prohibited by statute.
- E. Applicant fingerprint cards, RI-008, can be obtained from the MSP Warehouse.
- F. 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. [MCL 780.621](#) provides for the setting aside and sealing of certain criminal convictions. [MCL 712A.18e](#) provides for setting aside and sealing certain juvenile adjudications.
- B. Department work units shall fingerprint subjects on the state fingerprint card, RI-008, and return the card to the requester for submission to the CJIC.
- C. Questions concerning this statute shall be directed to the CJIC.
- D. 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.
- E. [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 LEIN policy rules, LEIN policies, and the Governor's Executive Order 1990-10.
- B. Requests for Criminal History Record Information other than those authorized by LEIN policy shall be directed to the CJIC.

Individuals requesting a personal record check to determine if criminal history record information is maintained at the CJIC shall be advised to submit a letter of request, specifying the requester's name, identifiers, fingerprints, and required fee to the CJIC.

29.1.11. PROCESSING CHALLENGES TO PUBLIC RECORDS

A. General Procedure

- (1) An individual who is the focus of a department record which he or she believes is incorrect has the right to seek correction of the record.
- (2) The request shall be accepted at any department work unit.
- (3) Requests must be in writing and include sufficient detail to enable the department to locate the contested document and confirm the validity of the allegation. The following information is needed for processing:
 - a. The proper name and date of birth of the individual who is the focus of the record.
 - b. The mailing address and telephone number of the individual.
 - c. The SID or FBI number, if available.
 - d. The incident number or arrest number of the contested record.
 - e. Documentation to verify that the department record is in error.
- (4) The identity of the individual seeking to have his or her record modified must be verified via fingerprints to ensure that the requestor is not an impostor attempting to modify information in another person's record.
 - a. The requestor may choose to be fingerprinted by the Michigan State Police or any other police agency.
 - b. If the requestor chooses to be fingerprinted by the Michigan State Police, a department member shall fingerprint the requestor using the applicant fingerprint card, RI-008.

B. Responsibilities of Work Site Commanders

Work site commanders shall:

- (1) Accept all requests for record challenges.
- (2) Assist the requestor by reviewing the written request to ensure that it contains sufficient information for processing.
- (3) Assist the requestor by ensuring the RI-008 is prepared and submitted.
- (4) Immediately forward the written request, RI-008, and evidence of error, if any, to the CJIC director.

C. Responsibilities of the CJIC

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

(3) Acting on the evidence found, the director of 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 and all recipients of this record over the previous six months shall be advised of the modification by the CJIC.

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

D. Appeal Process

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

(2) If the Director 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

Criminal History Record Information 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. Title 28

[Title 28 of the Code of Federal Regulations](#) Part 20 contains regulations issued by the United States Department of Justice pursuant to Sections 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended.

B. Criminal Justice Agency

"Criminal justice agency" is defined as courts, prosecutors, a government agency (or any subunit thereof) that administers criminal justice pursuant to a statute or executive order, and which 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" is defined as 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. Criminal History Record Information (CHRI)

CHRI means information about individuals by criminal justice agencies consisting of identifiable descriptions and notations of arrests, detention, indictments, information, or other formal criminal charges and any disposition arising therefrom, sentencing, correctional supervision, and release. All of this data is in a computerized storage and retrieval mode maintained by the CJIC.

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

NCIC/III is the national index of computerized criminal histories available via NCIC or 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.

G. The International Justice and Public Safety Network (Nlets)

29.2.2. AGENCIES SUBJECT TO TITLE 28 REGULATIONS

The Michigan State Police is the only agency in the state subject to the regulations of Title 28. However, a recipient of any CHRI maintained by this department becomes subject to the rules concerning dissemination and use of that record.

29.2.3. ACCOUNTABILITY FOR CHRI REQUESTS

Work units having terminal 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 LEIN terminal device 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 his or her agency, and any other data pertinent to the dissemination or use of the information.
- C. LEIN terminal requests for CHRI shall automatically be logged by the CJIC computer.
- D. District and division commanders, the Field Services 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 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 Unit (RRU).
- 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

Title 28 allows, but does not mandate, the release of CHRI to the news media. Requests for such information shall be forwarded to the Records Resource Section for processing.

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 Federal Bureau of Investigation's (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 Michigan Department of State Police (MSP) 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 his or her parent or guardian during the course of a User's lawful duties. The child and his or her parent or guardian may limit or withdraw consent at any time. If consent is withdrawn by either the child or his or her 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 his or her 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 federal CJIS Security Policy, the Michigan CJIS Security Addendum, 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. "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.
- F. "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.
- G. "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 Federal Bureau of Investigation's (FBI) [Criminal Justice Information Services \(CJIS\) Security Policy](#), particularly Policy Area 13, and the Michigan CJIS Security Addendum.
- B. The information within the SNAP databases is considered highly restricted personal information and PII 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 federal CJIS Security Policy, the Michigan CJIS Security Addendum, 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 personal information or PII 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 TATTO (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.
- 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.
- 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 his or her 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 Administrative Services Bureau (CJIC) and State Services Bureau (BID), in cooperation with the Office of the Director.

DIRECTOR