OFFICIAL ORDER
MICHIGAN STATE POLICE

Chapter: **Investigations and Enforcement Operations**

Subject: **07-07 – Mobile Fingerprint Identification**

Effective: April 19, 2022

Supersedes: Official Order 29, Section 29.3, dated February 26, 2021

Distribution: Department Members

PURPOSE: This Order 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.

07-07-1 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.

07-07-2 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 they 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.

07-07-3 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.

07-07-4 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.

07-07-5 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.

07-07-6 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.

DIRECTOR

Annual Review Responsibility: Biometrics and Identification Division

Accreditation Standards: CALEA TBD