PLANNING, RESEARCH AND DEPLOYMENT

TRANSMITTAL OF WRITTEN DIRECTIVE

FOR SIGNATURE OF: James E. Craig, Chief of Police

TYPE OF DIRECTIVE: Manual Directive 304.8

SUBJECT: MOBILE FINGERPRINT READER

ORIGINATED OR REQUESTED BY: Planning, Research and Deployment

APPROVALS OR COMMENTS:

APPROVED
JUL 11 2019
SECOND DEPUTY CHIEF
POLICE LEGAL ADVISOR

APPROVED
JUN 28 2019
ASSISTANT CHIEF
ADMINISTRATIVE OPERATIONS

AFTER THE DIRECTIVE IS APPROVED AND SIGNED, PLEASE RETURN TO PLANNING, RESEARCH AND DEPLOYMENT.
1301 Third Avenue, 7th Floor, Detroit MI 48226

4948

rdk
6-11

DETROIT POLICE DEPARTMENT
MANUAL

Series 300 Support Services	**Effective Date**	**Review Date** Three Years	**Directive Number** 304.8
Chapter 304 - Training			
Reviewing Office Office of Support Operations			☒ New Directive ☐ Revised
References			

MOBILE FINGERPRINT READER

304.8 - 1 PURPOSE

The purpose of this directive is to establish the guidelines for the issuance, training and use of the Mobile Fingerprint Reader (MFR).

304.8 - 2 POLICY

Mobile Fingerprint Readers are not intended to be the primary means of identifying subjects. The MFR is a tool used to assist members in the identification of an individual whose identity is in question when other means of identification are unavailable or questionable.

304.8 - 3 Definitions

304.8 - 3.1 Mobile Fingerprint Identification

A mobile fingerprint scanner is used in a mobile environment to attempt to identify an individual whose identity is in question. The scanned fingerprint images are compared to fingerprints stored in the Michigan Automated Fingerprint Identification System (AFIS) and the FBI Repository of Individuals of Special Concern (RISC) database.

304.8 - 3.2 Mobile Fingerprint Reader

A mobile 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.

304.8 - 3.3 Criminal Justice Information (CJI)

CJI is comprised of 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.

304.8 - 3.4 Authorized User

An individual employed as a law enforcement officer, or a *CJIS authorized* civilian employed by a criminal justice agency, whose agency is approved by the Detroit Police Department (DPD) to utilize MFRs.

304.8 - 3.5 Personally Identifiable Information (PII)

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.

304.8 - 4 Authorized Use of the Mobile Fingerprint Reader

The Mobile Fingerprint Reader shall only be used during the course of a user's lawful duties and when one of the following circumstances exists:

a. Consent of an Individual 17 Years of Age or Older

- Mobile identification (ID) may be used with consent of an individual 17 years 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 the use of Mobile Identification is solely based upon consent, use of the Mobile ID is not authorized and its use must stop immediately.

b. Consent of an Individual under 17 Years of Age and Parent or Guardian

- 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.

- 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 the Mobile ID is solely based upon consent, use of Mobile ID is not authorized and its use must stop immediately.

- 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 shall 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

- Mobile ID may be used without consent of individual of any age if one of the following circumstances exists:

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

- 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.

- Pursuant to a valid court order.

304.8 - 5 Identification Process

1. After fingerprint images are captured by the MFR, 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 Reader. 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 MFR:

   a. "Hit" – 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" – means no identification match was made.

   c. "Unable to Determine" – 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.

2. 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.

304.8 - 6 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, or as an entry on the enforcement member's daily Activity Log. At minimum, the documentation shall include the date, time, location and justification for utilizing Mobile ID.

304.8 - 7 Auditing and Penalties for Misuse

All Mobile ID use is subject to audit by the Civil Rights Division. All audit findings and administrative sanctions imposed are at the sole discretion of the commanding officer of the Civil Rights Division. Penalties that may be imposed include, but are not limited to, termination of a user's access to Mobile ID, termination of the mobile device's access to Mobile ID, and termination of agency-wide access to Mobile ID.

304.8 - 8 Disclosure and Use of Information

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 28.211-28.211.216, and most current CJIS Administrative Rules.

304.8 - 9 Discipline

Any violations to this policy specific to privacy, violation of use and private use shall be deemed egregious conduct. Furthermore, improper access, use or dissemination of PII or CJI obtained from Mobile ID may result in criminal penalties.