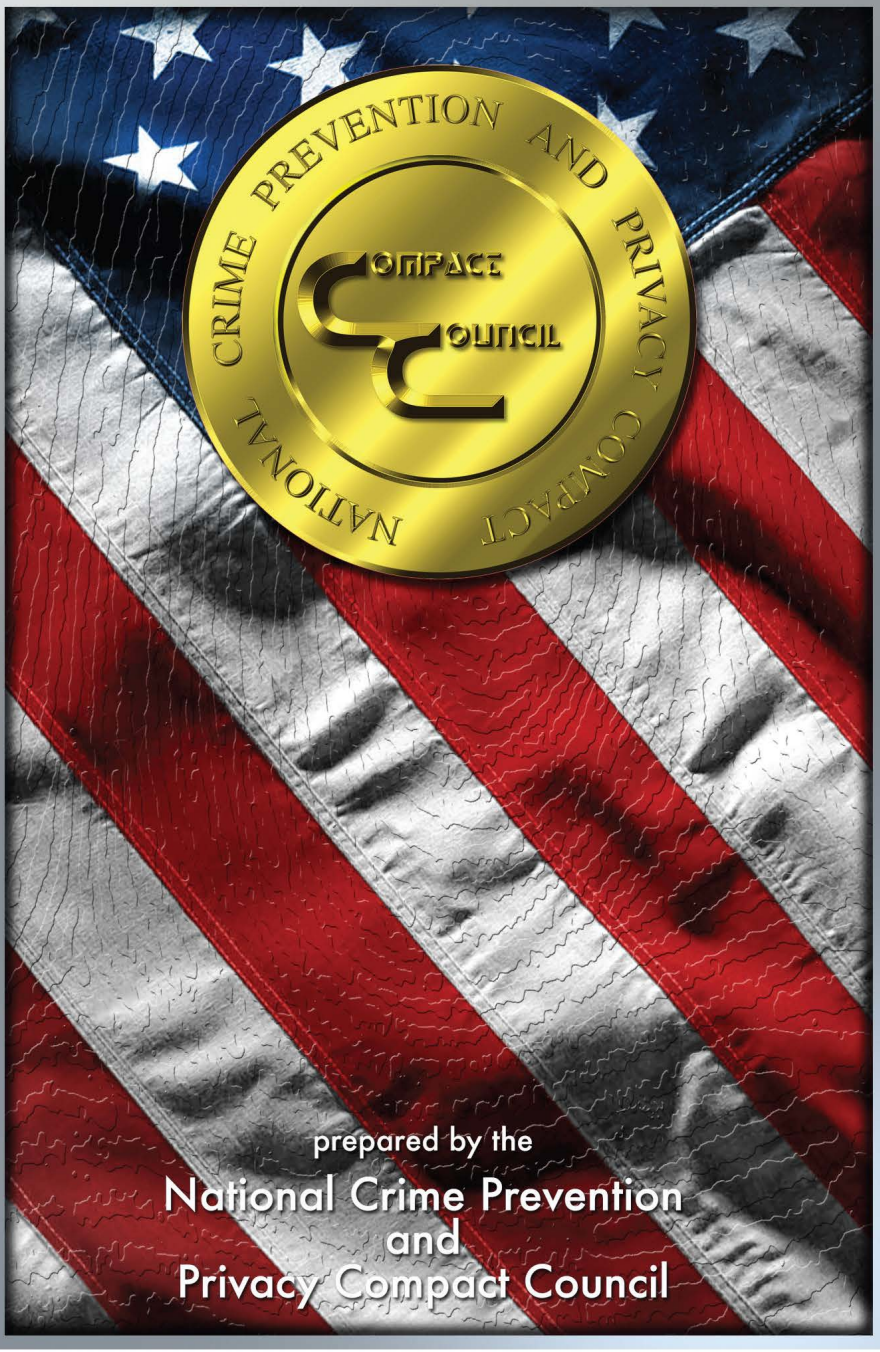
Identity Verification Program Guide



prepared by the

National Crime Prevention and Privacy Compact Council

The National Crime Prevention and Privacy Compact Council (Compact Council) is a15-member body of local, state, and federal governmental officials which prescribes system rules and procedures for the effective and proper operation of the Interstate Identification Index (III) for noncriminal justice purposes.

In recent years, the demand for fingerprint-based background checks for noncriminal justice purposes has increased. Fingerprinting agencies and contractors alike have expressed concern that applicants with a criminal history record may have someone pose as the applicant for fingerprinting purposes. In response to these concerns, the Compact Council prepared this guide for voluntary use in the development of policy, procedures, and practices for applicant identity verification.

Factors to Consider

(For the purpose of this guide, "agency" will refer to any agency or contractor responsible for the capture and/or submission of fingerprints for noncriminal justice purposes.)

In the course of establishing an identity verification program, agencies may choose to consider the following factors:

- Clearly define and document policy, procedure, and practices. Document what is to be accomplished and how it is to be performed.
- Review current business policy, procedure, and practices regarding verification, training, legal obligations, and privacy implications that may be incorporated into a program.
- Develop an understanding of the use of various biometric-based systems.

Preliminary Considerations

Coordination with the State Repository

Since the state repository manages the processing of fingerprint submissions to the FBI, it is suggested that appropriate coordination and liaison be established at that level as a preliminary step toward an identity verification program.

Fingerprinter Certification

Another preliminary consideration for states may be the enacting of a state statute establishing a certification process that qualifies the employees capturing the applicant's fingerprints. Additionally, if the statute were compliant with Public Law 92-544, a state and federal fingerprint-based background check could be performed on the individuals certified to take fingerprints.

Policy, Procedures,

In developing an identity verification program, the Compact Council suggests establishing written policy, procedures, and practices. The following guide may be helpful in the process.

- Determine Policy, Procedures, and Practices
- Create an Identification Validation Guide
- Create Chain of Custody Procedures

Determine Policy, Procedures and Practices

Policy, Procedures, and Practices may include:

A. Training in the capture of fingerprints (rolled or flats, and hard copy or livescan).

B. Certification of employees performing duties under the scope of the identity verification program, which may include recognizing and validating authorized identification forms, identification documents, and source documents for identity confirmation.

C. Security considerations:

1. Train employees to recognize and properly utilize the security features of the various forms of identification presented. These features include biometric like photographs and machine-readable technology such as magnetic strips and 2D/3D barcodes.

2. Assign a unique identification number to each employee to be included with each fingerprint submission.

Primary and Secondary Identification

Currently most agencies request some type of photo identification card as one method for verifying an individual's identity. The Compact Council suggests agencies accept only current, valid, and unexpired photo identification documents.

As a primary form of photo identification, the following documents may be presented by an applicant when being fingerprinted:

- State-issued driver's license*
- U.S. Passport or U.S. Passport Card
- Federal Government Personal Identity Verification Card (PIV)
- Uniformed Services Identification Card
- Department of Defense Common Access Card
- Foreign Passport with Appropriate Immigration Document(s)
- USCIS - Permanent Resident Card (I-551)
- USCIS - Employment Authorization Card (I-766)
- Federal, state, or local government agency ID card with photograph
- U.S. Coast Guard Merchant Mariner Card
- Canadian driver's license

* *For those applicants without a driver's license, a state identification card may be presented if the state's identification card standards are the same as for the driver's license.*

However, in the absence of a primary identification, applicants may provide at least 2 secondary identification documents including:

- State Government Issued Certificate of Birth
- U.S. Tribal or Bureau of Indian Affairs Identification Card
- Native American tribal document
- Social Security Card
- Court Order for Name Change/Gender Change/ Adoption/Divorce

- Marriage Certificate (Government Certificate Issued)
- U.S. Government Issued Consular Report of Birth Abroad
- Draft record
- School ID with photograph
- Certificate of Citizenship (N-560)
- Replacement Certificate of Citizenship (N-561)
- Certificate of Naturalization (N-550)
- Replacement Certificate of Naturalization (N-570)

Secondary Identification Data Support Documents

When validating the authenticity of secondary identification documents and forms, the data and information may be supported by at least two of the following current documents:

- Utility Bill (Address)
- Jurisdictional Voter Registration Card
- Vehicle Registration Card/Title
- Paycheck Stub with Name/Address*
- Jurisdictional Public Assistance Card
- Spouse/Parent Affidavit

* *Financial information may be redacted by the individual.*

Additional Identification Data Support Methods

To further support the validation of the original identification documents, the agency may choose any or all of the following methods to validate the authenticity of the documents:

- Physically examine the applicant's photo on the identification form/card. Visually compare the photo with the applicant in person.

- Compare the physical descriptors of the applicant to the documentation provided by the applicant (i.e. height, weight, hair and eye color, age, etc.).

- Request the applicant to verbally provide date of birth, address, etc., and check this against the identification forms used.

- Check the applicant's signature in person with that on the identification form.

- Ensure that the identification form has not been altered in any manner.

- If available, verify that the machine readable data matches the data on the card when it is scanned.

When an agency has a reason to believe an applicant has presented fraudulent information, agency personnel should contact local law enforcement. No attempt should be made to detain or pursue the person.

Create Chain of Custody Procedures

An agency may employ a process to protect the integrity of the applicant's fingerprints when they are forwarded to the state identification bureau and/or the FBI. The following information provides a guide to developing a chain of custody process:

A. Establish provisions for the agency to manage both manually and electronically captured fingerprints.

B. Establish an agency tracking system (applicant log) using the employee's name or some other method of identifying the individual capturing the fingerprints and verifying the applicant's identity.

C. Establish procedures that document the type(s) of identification used by the applicant.

D. When possible, electronic fingerprint submissions should be used, thus eliminating the return of the fingerprint card to the applicant. However, in those instances when the fingerprints must be returned to the applicant, the agency should establish procedures that use specially sealed envelopes, agency specific stamps, etc. when forwarding the applicant's manually captured fingerprints.

E. Implement the use of form(s), which may include the:

1. Date of fingerprinting
2. Reason for fingerprinting
3. Printed name, signature, and/or identification number of the employee taking the fingerprints
4. Name of employee's supervisor
5. Supervisor's signature
6. Address of agency to receive fingerprints
7. Name of agency and physical address where fingerprinting was performed
8. Type of fingerprint capture (rolled ink, flat ink, live scan, etc.)
9. Applicant's consent for fingerprinting
10. Type of ID verified (Driver's License #/State/Expiration Date)

For further information, please visit the Compact Council website at:

www.fbi.gov/about-us/cjis/cc/cc

Fingerprint Fraud Scenarios

1. The following scenarios illustrate how an applicant attempted and successfully circumvented the fingerprinting process in order to obtain a position of trust and the importance of verifying the individual's identity, as well as maintaining the chain-of-custody:

- An individual applied for, and successfully obtained, a position of trust as a teacher within a school district, after having another individual go to the sheriff's office and provide his fingerprints. The prospective teacher also utilized his father's name, which was the same as his. The fingerprints were subsequently submitted to the State Identification Bureau for a background check. Two years later, the falsified fingerprints were discovered when the teacher was arrested for criminal trespass and window peeping. It was also discovered the teacher had a prior arrest and conviction for simple assault and a sexual battery arrest which resulted in a misdemeanor assault conviction. As a result, the individual's employment was terminated. Subsequently, the individual who had submitted the falsified fingerprints was also arrested for fraudulent activity.

- An applicant with a disqualifying out-of-state arrest applied for a teacher certificate and persuaded a student to provide the applicant her fingerprints. The fingerprints were submitted and the applicant was able to obtain a teaching certificate. The student subsequently was arrested and the fingerprints hit on her own fingerprints that were in the state rap back system. When the Department of Education received the rap back notification, they discovered that the mug shot did not match the teacher enrolled in rap back. An investigation revealed identity fraud and the case was turned over for criminal prosecution of both the teacher applicant and the student. In this instance rap back prevented a disqualified individual from having continued access to a vulnerable population.

2. The following scenario illustrates how an applicant attempted to circumvent the fingerprinting process in order to obtain a position of trust, but due to the vigilance of the fingerprinting vendor, the hiring agency was able to successfully prevent the individual from obtaining the position.

- An individual applied for a health care worker position. Due to the fact that she had a criminal history record, she requested her roommate be fingerprinted on her behalf. Unbeknownst to her, the roommate also had a record. However, the fingerprinting agency verified the applicant's identification and determined that the photo/biographic identification did not match the applicant's identity. The fingerprint vendor notified the Department of Health (DPH) that the applicant did not match the identification submitted. Subsequently, both the applicant and the individual that agreed to submit the false fingerprints were arrested and charged. Due to verification of the identification, the DPH was able to detect fingerprint fraud and prevent a convicted felon from obtaining a position of trust as a health care worker.

Federal Legislation and Other Documents Pertinent to this Guide:

42 U.S.C. § 14616

Public Law 109-13, also referred to as the REAL ID Act
(The Emergency Supplemental Appropriations Act for Defense,
the Global War on Terror, and Tsunami Relief Act, May 11, 2005)

HSPD-12 (Homeland Security Presidential Directive - 12)

Revised 2014 by the National Crime Prevention and Privacy Compact Council