

IMPORTANT NOTICE: Completion of this form is necessary for licensure/employment under provision set forth within the Illinois Compiled Statutes or other related Federal laws. Disclosure of this information is VOLUNTARY. However, failure to comply may result in the denial of your application.

## IDENTITY VERIFICATION CERTIFYING STATEMENT

# OOS-FP

Pursuant to Title 68 Part 1240.535 of the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 Rules, fingerprint vendors are required to confirm identity of the individual seeking to be fingerprinted. This identity verification form must be completed for out-of-state residents applying for licensure/employment in the State of Illinois. This form will be utilized to confirm the personal identifying information being placed on the Illinois State Police (ISP) Fee Applicant fingerprint card, form number ISP-404. The out-of-state agency chosen to take your fingerprints, must complete this form, as written confirmation that a valid government issued drivers license or State ID was presented and that the identification provided, belongs to the individual being fingerprinted.

**Instructions:** This form must be submitted, along with a manual Fee Applicant fingerprint card to which your fingerprints have been applied, to a licensed live scan fingerprint vendor in the State of Illinois possessing "Scan Card" capability to ensure electronic transmission of the Fee Applicant fingerprint card. The electronic transmission of fingerprints to the ISP is mandated pursuant to Title 20 Part 1265 "Electronic Transmission of Fingerprints". **The manual submission of fingerprints to ISP is no longer acceptable.** Once your fingerprints have been taken, a signed original of this form must be attached to your Fee Applicant fingerprint card and submitted to an Illinois licensed live scan fingerprint vendor. As well, an additional copy may be required to be submitted to the requesting State Agency along with any additional application or required documentation specified by the State Agency.

### Section 1 Applicant Information (All fields mandatory)

LAST NAME:	FIRST:	MIDDLE:	PHONE NUMBER:
MAIDEN NAME/GIVEN SURNAME:		POSITION / REASON FINGERPRINTED: (NURSE/DOCTOR/SECURITY GUARD, ETC)	
ADDRESS: (STREET/CITY/STATE/ZIP)		DATE OF BIRTH:	SOCIAL SECURITY NUMBER:

### Section 2 Certifying Agency Taking Fingerprints (Include TCN from Fee Applicant card)

AGENCY NAME:	TCN: FRM
DATE FINGERPRINT TAKEN: / /	CONTACT PHONE NUMBER: ( ) -
PRINTING AGENT'S NAME: LAST	FIRST



I have compared the government issued identification presented by the applicant and attest that to the best determination, I have fingerprinted the same individual. (Must be checked to certify)

PRINTING AGENT'S SIGNATURE:

## Illinois Live Scan Fingerprint Vendor Information

### Section 3 Fingerprint Vendor Agency Name

LIVE SCAN FP AGENCY NAME: <b>Biometric Impressions Corp</b>	
REQUESTING STATE AGENCY:	REQUESTING STATE AGENCY ORI:
DATE FINGERPRINTS SUBMITTED TO ISP: / /	COST CENTER USED: <b>5051</b>

TCN #: LS

## "Striving to be the Leader of Fingerprinting Services"

Visit any of our multiple locations throughout Illinois

Phone: 833-4 BIOIMP (833-424-6467) | Fax: (888) 745-0247

ILDPR License No. - 262.000039

[www.biometricimpressions.com](http://www.biometricimpressions.com) | E-Mail: [info@biometricimpressions.com](mailto:info@biometricimpressions.com)

## BIPA Retention Policy



\*Authority: The FBI's acquisition, preservation, and exchange of fingerprints and associated information is authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include Federal statutes, State statutes pursuant to Pub. L. 92-544, Presidential Executive Orders, and federal regulations. Providing your fingerprints and associated information is voluntary; however, failure to do so may affect completion or approval of your application.

\*\*Principal Purpose: Certain determinations, such as employment, licensing, and security clearances, may be predicated on fingerprint-based background checks. Your fingerprints and associated information/biometrics are being collected, stored, used, and disclosed to the Illinois State Police ("ISP"), Illinois Bureau of Identification ("BOI") and/or FBI for purposes of conducting those background checks, and may be provided to the employing, investigating, or otherwise responsible agency, and/or the FBI for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification ("NGI") system or its successor systems (including civil, criminal, and latent fingerprint repositories), the BOI's Automated Fingerprint Identification System ("AFIS"), the Criminal History Record Information system ("CHRI") and/or the Automated Biometric Identification System ("ABIS"), or their successor systems (including civil, criminal, and latent fingerprint repositories), or other available records of the employing, investigating, or otherwise responsible agency. The FBI, ISP, and BOI, may retain your fingerprints, photograph and associated information/biometrics in NGI, AFIS, CHRI and/or ABIS after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI, AFIS CHRI and/or ABIS.

\*\*\*Routine Uses: During the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in NGI, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses. In addition, during the processing of this application and for as long thereafter as your fingerprints and associated information/biometrics are retained in AFIS, CHRI and/or ABIS, your information may be disclosed pursuant to your consent, and may be disclosed without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time, including the Routine Uses for AFIS, CHRI and/or ABIS, and the BOI and ISP's Blanket Routine Uses. Routine Uses include, but are not limited to, disclosures to: employing, governmental or authorized nongovernmental agencies responsible for employment, contracting, licensing, security clearances, and other suitability determinations; local, state, tribal, or federal law enforcement agencies; criminal justice agencies; and agencies responsible for national security or public safety.

\*\*\*\*Retention: BioMetric Impressions Corporation (BIC) shall retain and destroy Your fingerprints and biometric data consistent with BIC's Biometric Data Retention and Destruction Policy ("Retention Policy"), which was provided to You with this Consent Form. By signing below, you acknowledge Your receipt of and opportunity to review the Retention Policy. According to the Retention Policy, BIC retains fingerprint images and biometric data for 45 days from the date of receipt, capture or card scan date, at which point they will be permanently destroyed, unless BIC is required by government contract to retain them for a longer period of time. A copy of BIC's Retention Policy is available to the public at any BIC physical location, via the QR code at the bottom of this form, and on BIC's website at: <https://www.biometricimpressions.com/compliance/>.

\*\*\*\*\*Consent: By signing below, I acknowledge and hereby authorize the collection, storage, use, and disclosure of my fingerprint images and/or information based on or derived from my fingerprint images, and the release of any criminal history record information that may exist regarding me from any agency, organization, institution, or entity having such information on file. I understand that my fingerprints may be retained and will be used to check the criminal history record information files of the ISP, BOI and/or the FBI, to include but not limited to civil, criminal and latent fingerprint databases. I also understand that if my photo was taken, my photo may be shared only for employment or licensing purposes. I further understand that I have the right to challenge any information disseminated from these criminal justice agencies regarding me that may be inaccurate or incomplete pursuant to Title 28 Code of Federal Regulation 16.34 and Chapter 20 ILCS 2630/7 of the Criminal Identification Act.

Applicant Signature: \_\_\_\_\_ Date: \_\_\_\_\_

Legal Last Name/Apellido Legal: \_\_\_\_\_

Legal First Name/Primer Nombre Legal: \_\_\_\_\_

Middle Initial/Inicial del Segundo Nombre: \_\_\_\_\_

SSN: \_\_\_\_\_ Date of Birth/Fecha de Nacimiento: \_\_\_\_/\_\_\_\_/\_\_\_\_

Email: \_\_\_\_\_ Telephone: \_\_\_\_\_

\*\*\*\*\*I acknowledge that I have taken a picture of this consent form with my personal cell phone, and this will act as my copy of the consent form.

Applicant Signature: \_\_\_\_\_ Date: \_\_\_\_\_

## Official Use Only

Purpose Code: \_\_\_\_\_ ORI: \_\_\_\_\_

Applicant TCN: \_\_\_\_\_

ID Type: \_\_\_\_\_ ID State: \_\_\_\_\_ No.: \_\_\_\_\_

Date: \_\_\_\_\_ Technician: \_\_\_\_\_

## Payment Method

Square

Check#: \_\_\_\_\_

Invoice

Customer Code: \_\_\_\_\_

Notes: \_\_\_\_\_

# BIOMETRIC IMPRESSIONS CORP.'S BIOMETRIC DATA RETENTION AND DESTRUCTION POLICY

## 1. Introduction

### 1.1 Background

BioMetric Impressions Corp. is a licensed fingerprint vendor in Illinois. Section 1240.535(c)(8) of the Illinois Administrative Code provides: "A licensed fingerprint vendor must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying identifiers and other biometric information when the initial purpose for collecting or obtaining the identifiers or information has been satisfied or after 3 years from the individual's last interaction with the licensed fingerprint vendor, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines" (the "Regulation"). This Policy is made pursuant to and in accordance with the Regulation.

### 1.2 Definitions

The Regulation generally tracks language in the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (the "Act"). The Regulation does not define the terms "identifiers" and "biometric information," but the Act defines the terms "biometric identifier" and "biometric information." BioMetric Impressions therefore construes the phrase "identifiers and other biometric information" as it appears in the Regulation to be consistent with the definitions in the Act. Accordingly, whenever used within the Policy, unless otherwise clearly documented:

- (1) "Biometric data" means "biometric identifiers" and "biometric information."
- (2) "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.
- (3) "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.
- (4) "CMS Contract" means the contract between BIC and CMS titled State of Illinois Contract, Central Management Services Fingerprinting and Photographic ID Services, Number 19-416CMS-BOSS4-P-4770, effective October 26, 2018.
- (5) "Government contract" means an agreement between BioMetric Impressions, on the one hand, and any federal, state, or local governmental entity, on the other hand, pursuant to which the government pays BioMetric Impressions for fingerprinting services, including, without limitation, the CMS Contract.
- (6) "Identifiers and other biometric information" means biometric identifiers and biometric information.

## 2. Retention Policy

Unless otherwise obligated by Government contract to maintain fingerprint images for a different period of time, BioMetric Impressions retains identifiers and other biometric information, including fingerprint images, for up to 45 days from the date of receipt, fingerprint capture or card scan date.

If a collection or transmission error results in the need for a new set of fingerprint images to be taken, a new fingerprint inquiry transaction is created with a new date of fingerprint capture, which in turn starts the 45-day retention date from the revised date of fingerprint capture.

When obligated by Government contract to retain fingerprint images for longer than 45 days, BioMetric Impressions programmed its database to retain the digital images to the specified contractual requirements. Such electronic retention relies on the purpose for which the fingerprints were captured. The CMS Contract is an example of a Government contract pursuant to which BioMetric Impressions is obligated to retain fingerprint images for longer than 45 days.

BioMetric Impressions recognizes that the requirements of certain Government contracts may appear to conflict with the Regulation and the retention time frame described above, but it believes the intent of the Regulation is not to conflict with governmental contractual requirements and can be reconciled by the fact that the initial purpose of the contractual requirement has not been met and the governmental entity is relying upon the fingerprinting agency for archival of its records. Additionally, the Act specifically provides that it does not apply to contractors of State or local governments when said contractors are working for a government agency or local unit of government, which is consistent with the conclusion that the Regulation is not intended to restrict a government contractor from retaining records for longer than three years if required to do so by the Government contract. Accordingly, a retention period of more than three years is warranted and permissible in certain circumstances, as specified by the applicable government contract.

## 3. Permanent Destruction Policy

### 3.1 Electronic Documents

Upon the expiration of the retention period for given identifiers and other biometric information, BioMetric Impressions securely deletes such identifiers and other biometric information. Through that deletion process, the identifiers and other biometric information are no longer accessible and permanently destroyed on the applicable storage drive and/or server space.

### 3.2 Physical Documents

Some identifiers and other biometric information may be received in paper form, e.g., fingerprint cards. Those identifiers and other biometric information are converted into an electronic/digital format. Thereafter the physical documents are placed in a file for a period of up to 30 days. On or before such 30 days expires, the physical documents are placed in a secure shred bin.

## 4. Exceptions to Policy

Absent a valid warrant or subpoena issued by a court of competent jurisdiction or other applicable law or legal requirement, BioMetric Impressions will comply with this Policy.

## 5. Roles and Responsibilities

BioMetric Impressions has assigned its President to be responsible for overseeing and implementing the Policy.

## 6. Questions and Copies

This policy shall be available to the public and be provided upon request. Questions related to the Policy, including requests for the most recent version of the Policy, should be directed to:

Attn: President  
BioMetric Impressions  
188 W Industrial Dr. Suite 101  
Elmhurst, IL 60126  
e-Mail: [compliance@biometricimpressions.com](mailto:compliance@biometricimpressions.com)

