

PRIVACY IMPACT ASSESSMENT

**Fieldprint, Inc.
(Fieldprint)**

December 2015

FDIC External Services

Table of Contents

[System Overview](#)

[Personally Identifiable Information \(PII\) - Fieldprint](#)

[Purpose & Use of Information - Fieldprint](#)

[Sources of Information - Fieldprint](#)

[Notice & Consent](#)

[Access to Data - Fieldprint](#)

[Data Sharing](#)

[Data Accuracy - Fieldprint](#)

[Data Security - Fieldprint](#)

[System of Records Notice \(SORN\)](#)

[Contact Us](#)

System Overview

In support of the Federal Deposit Insurance Corporation's (FDIC's) Strategic Plan Objective of acquiring and retaining only trustworthy employees and contractors, and as required by Federal and FDIC employment suitability requirements, the FDIC Division of Administration (DOA) Security & Emergency Preparedness Section (SEPS) performs on-boarding processes that include fingerprinting and receipt of preliminary background investigation applications.

DOA SEPS has contracted through the Federal Bureau of Investigation (FBI) via an Other Direct Cost (ODC) line item with Global Resource Solutions to secure the services of Fieldprint, Inc., an authorized channeler¹. Fieldprint handles the fingerprinting process from collection through transmission to the FBI, ensuring that information is collected in a secure, timely, and convenient manner for employees, applicants, and contractors. The FBI, in turn, processes the digital fingerprints through their Criminal Justice Information Services Division (CJIS) and returns the results to Fieldprint. Fieldprint maintains the results in a secure, FDIC-specific section of their website for review and retrieval by pre-approved representatives of the FDIC. The fingerprints are digitally collected via a Livescan device, which is a digital scanner that will record fingerprints without the use of ink; the use of a Livescan device helps to ensure that all fingerprints collected are classifiable, resulting in a true search of the FBI's criminal indices. A digital fingerprint is a person's analog fingerprint converted into a binary machine-readable format; digital fingerprints cannot be reconstructed from any other digital fingerprints. This is helpful in identifying applicants with felony arrest records and also mitigates potential attempts to use false identification to obtain employment with the FDIC.

Per the FDIC's instructions, employees being reinvestigated², employee applicants, and prospective contractors or subcontractors (collectively referred to as "subjects" or "applicants" throughout this document) must make arrangements to be fingerprinted via the Fieldprint website (www.fieldprint.com). Fieldprint will issue to DOA SEPS a code for the applicant to use when scheduling his/her fingerprint appointment on the Fieldprint website. Through the use of this code, any and all charges for the fingerprinting will be sent to Global Resource Solutions for payment coordination with FDIC. There is no charge levied against any subject or applicant. FDIC has modified Global Resource Solutions, Inc.'s (GRS) contract to assign GRS as third-party administrator of the payments of Fieldprint expenses for these fingerprint services.

Based on the applicant's zip code location, the individual is referred to his/her local Fieldprint fingerprinting office. Applicants must have two valid forms of government-issued photo identification (i.e., Driver's License, Passport) with them when they arrive for fingerprinting. Fingerprints are collected via Livescan and securely transmitted to the FBI Integrated Automated Fingerprint Identification System (IAFIS)³ for processing against criminal indices. Within 48 hours of fingerprinting, the results of the FBI check are available for FDIC's viewing and retrieval on the Fieldprint secure site. FDIC will designate a select group of DOA SEPS Personnel

¹ A channeler is a title bestowed by the FBI on those authorized to process fingerprints on behalf of the FBI to collect and transmit applicant fingerprints during the FDIC pre-clearance and background investigation process.

² In the future, Fieldprint may also be used for fingerprinting FDIC contractors who are being reinvestigated.

³ IAFIS is a national fingerprint and criminal history system maintained by the FBI.

Security Unit (PSU) personnel to have password access via a web browser to view and retrieve available reports.

Fieldprint retains individual criminal history records until the FDIC retrieves them at which time the digital record will be destroyed per FDIC requirements. The FBI requires Fieldprint to maintain a log of who has been fingerprinted for 365 days. This audit log will contain:

- Name of the individual
- Submission events (both transmission and receipts)
- Data Access (i.e., a note about what documents/items were viewed such as driver's license, passport, Social Security number, orders)
- Summary of Email Communications (i.e., a narrative with the date and nature of communication, such as request to reschedule appointment)
- Password change attempts (successful and unsuccessful)
- Logon attempts (successful and unsuccessful)
- Permission changes for criminal history record information (CHRI) access functionality (add and revoke)

Personally Identifiable Information (PII) - Fieldprint

Fieldprint collects PII that may include: full name and any previous or current aliases; signature; home address; email address; employment information; criminal information; citizenship, Social Security number (SSN); date of birth (DOB); place of birth POB; sex; race; height; weight; eye color; hair color; and biometric identifiers (e.g., fingerprints). It is a mandatory requirement of the FBI to provide the aforementioned biometrics in order for the FBI to process the request. The information is collected at the time the applicant registers for the fingerprint appointment, and it is validated at the time of fingerprinting.

Purpose & Use of Information - Fieldprint

The PII is employed for those instances or aspects of the FBI records review that are name-based only. Under the best of circumstances, a certain percentage of individuals will provide fingerprints that are not classifiable. In those instances, a name check of the FBI Integrated Automated Fingerprint Identification System (IAFIS)⁴ is performed with the PII serving as the differentiator when record hits result that may or may not be the applicant.

Sources of Information - Fieldprint

FDIC Applicants, Prospective Contractors and Employees at Time of Reinvestigation: FDIC applicants, prospective contractors and employees at time of reinvestigation provide the PII information identified above to Fieldprint.

⁴ IAFIS is a national fingerprint and criminal history system maintained by the FBI.

Federal Bureau of Investigation (FBI): Criminal history information in the form of an FBI record is obtained via a secure submission of the digital fingerprints to FBI CJIS where it is run against criminal history records. The results are securely transmitted back to Fieldprint and held in the FDIC section of the secure Fieldprint database.

Notice & Consent

Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information. At the onset of the pre-clearance process, the applicant is issued a written Privacy Act advisement informing them that providing PII data and submitting to fingerprint scanning are voluntary; however, this information is necessary in order to complete the clearance process and render a final decision regarding the applicant's suitability for employment. Therefore, it is understood that further processing of the applicant's background investigation forms and affiliation with the FDIC are not possible without the cooperation of the applicant.

Access to Data - Fieldprint

Fieldprint Staff, Subcontractors, and/or Systems: When FDIC applicants/subjects arrive at a Fieldprint location for fingerprinting, authorized Fieldprint Field Technicians review their government-issued identification cards (driver's license, passport), collect their digital fingerprints via Livescan, and securely transmit this data to IAFIS for processing against criminal indices. The data is transmitted to IAFIS via a secure, direct link. FBI results are returned via the same direct link, and Fieldprint maintains the results in their secure network/system until the results are retrieved by FDIC. The FBI requires Fieldprint to maintain an activity log for 365 days that is a simple chronology of who was fingerprinted and when. Fieldprint personnel do not review the results of FBI checks; this is an automated process. However, authorized Fieldprint system administrators have access to the entire Fieldprint system (and all data contained therein) for purposes of system maintenance and troubleshooting. Refer to the "Data Security" section for information about the administrative and technical controls that Fieldprint has implemented to adequately safeguard PII in its care.

FDIC Personnel and/or FDIC Systems/Applications: Authorized employee and contractor personnel within the Personnel Security Unit (PSU) of DOA SEPS will receive the results of the FBI fingerprint check for use, in part, for rendering a due diligence determination on background investigation cases for FDIC applicants and for re-investigating current FDIC employees. The results will be stored in a secure fashion in the PSU's shared drive and Documentum. Authorized PSU personnel will also enter the fingerprinting date and fact there of in FDIC's Background Investigation Tracking System.

Other Non-FDIC Entities/Parties and/or Non-FDIC Systems/Applications: Through the use of the FDIC code, any and all charges for the fingerprinting will be sent to Global Resource Solutions for payment coordination with FDIC. There is no charge levied against any subject or applicant.

The process works as follows:

- On a monthly basis, an invoice is forwarded by Fieldprint via email to the FDIC Chief, Security Operations via the Senior Program Manager for GRS. The GRS Senior Program Manager and his staff first perform an audit of the invoice to ensure the charges for the month are accurate.
- The Invoice contains the following information relative to each examination for which there is a billing:
 - The submission date for each examination
 - The order number for each examination
 - Each applicant's first and last name
 - A breakdown of the fee charges for each examination
 - Fee totals
- Upon validating the content and accuracy of the Invoice, it is presented to the FDIC Chief, Security Operations for his approval in writing. This approval is chronicled via a notation and signature on the front of the presented invoice.
- Once the FDIC Chief, Security Operations has approved the Fieldprint Invoice, it is forwarded to the GRS Controller for disbursement of funds to Fieldprint.
- The original of the Invoice approved by the FDIC Chief, Security Operations is maintained by the GRS Senior Program Manager. Copies are maintained by the FDIC Chief, Security Operations and the GRS Accounting Department.

Federal, State, and/or Local Agencies: Authorized Fieldprint staff will securely transmit applicants' PII data and digital fingerprints to IAFIS, which is a national fingerprint and criminal history system that provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses. Refer to the "Sources of Information" section above for additional information about how data is transmitted to IAFIS. Refer to the Department of Justice/FBI Privacy Impact Assessments (PIAs) website for more information about IAFIS: <http://www.fbi.gov/foia/privacy-impact-assessments/departement-of-justice-federal-bureau-of-investigation>.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

System Name	System Description	Type of Information Processed
N/A	N/A	N/A

Data Accuracy - Fieldprint

Data is collected directly from individuals. As such, the FDIC and Fieldprint rely on the individuals to provide accurate data.

In addition, each person to be fingerprinted must present two forms of identification to validate their identity. The fingerprints are collected on Livescan equipment, thereby ensuring a true technical fingerprint search of the criminal history records of the FBI. Finally, a background investigation is conducted on the applicant.

Data Security - Fieldprint

Fieldprint is an authorized channeler on behalf of the FBI and, as such, undergoes rigorous oversight by the FBI. The FBI Security and Management Control Outsourcing Standards for Channelers (Outsourcing Standard) provides an overview of the FBI's requirements. As part of the FBI's Outsourcing Requirement, Fieldprint must undergo a thorough security review by the FDIC. FDIC employs an assessment to determine and/or verify that Fieldprint has appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data.

Fieldprint is subject to periodic compliance reviews by FDIC and the FBI. Per the contract, scheduled and unannounced inspections and assessments of Fieldprint's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements.

The FBI conducts criminal history checks on all Fieldprint personnel associated with the fingerprint channeling process. The FBI also requires Fieldprint, as one of its authorized channelers, to adhere to the Outsourcing Standard, which stipulates adequate security and integrity controls for criminal history record information while under the control or management of Fieldprint. Adequate security as defined in the Outsourcing Standard, consistent with Office of Management and Budget (OMB) Circular A-130, as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." The intent of the Outsourcing Standard is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI CJIS Security Policy), as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

The Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the CHRI and any other data collected/maintained by Fieldprint on behalf of agencies are not compromised. As such, Fieldprint's standard security program must encompass adequate site security, dissemination restrictions, personnel security, system security, and data security. Additionally, as noted above, Fieldprint is subject to periodic compliance reviews by FDIC and the FBI.

Within FDIC, the Fieldprint Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

Additionally, Fieldprint is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and Fieldprint has designated an account executive to have overall accountability for ensuring the proper handling of data by Fieldprint personnel who have access to the data. All Fieldprint personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as Fieldprint's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data.

Fieldprint must comply with the Incident Response and Incident Monitoring contractual requirement.

System of Records Notice (SORN)

Fieldprint operates under the FDIC Privacy Act SORN 30-64-0015, *Personnel Records*.

Contact Us

To learn more about the FDIC's Privacy Program, please visit:
<http://www.fdic.gov/about/privacy/>.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the [FDIC Privacy Program Contacts](#). You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.

