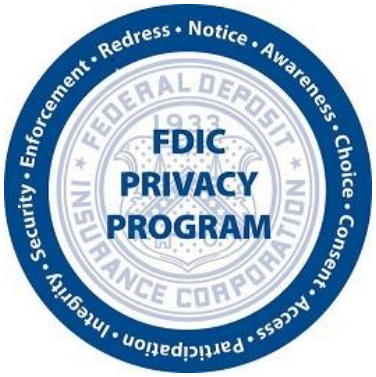
FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Threshold Analysis (PTA) and/or Privacy Impact Assessment (PIA)

for

Fieldprint, Inc.



Date Approved by Chief Privacy Officer (CPO)/Designee: 1/28/2019

PTA/PIA TEMPLATE VERSION 1.9 – August 2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

Within the Federal Deposit Insurance Corporation (FDIC), the Cyber Fraud and Financial Crimes (CFFC) Section of the Division of Risk Management Supervision (RMS) is responsible for conducting background investigations (BIs) on individuals in connection with applications and notices submitted to the FDIC, such as applications for Federal Deposit Insurance (FDI), Notices of Acquisition of Control, applications subject to Section 19 of the FDI Act, and notices subject to Section 32 of the FDI Act. These investigations are conducted to determine if those proposed have the experience, competence, integrity, character, financial ability, and willingness to direct and/or lead a bank's affairs in a safe, sound, and legal manner.

RMS and the FDIC Division of Administration (DOA) Security & Emergency Preparedness Section (SEPS) entered into a contract with Fieldprint, Inc. in February 2018 to collect and transmit subject fingerprints to the Federal Bureau of Investigation (FBI). Fieldprint is an "FBI-approved channeler," a title bestowed by the FBI on select vendors authorized to serve as a conduit for submitting fingerprints to the FBI and receiving the FBI criminal history record information (CHRI) on behalf of authorized recipients for noncriminal justice purposes. Fieldprint handles the fingerprinting process from collection through transmission to the FBI, ensuring that information is collected in a secure, timely, and convenient manner. 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 secure 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 individuals with felony arrest records and also mitigates potential attempts to use false identification to obtain employment.

Per the FDIC's instructions, Financial Institution applicants (referred to as "subjects" or "applicants" throughout this document) must make arrangements to be fingerprinted via the Fieldprint website (https://schedule.fieldprint.com). Fieldprint will issue a code to RMS 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 FDIC for payment.

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)[1] for processing against criminal indices. Refer to the Department of Justice/FBI Privacy Impact Assessments (PIAs) website for more information about IAFIS: https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/firs-iafis.

SECTION II – DATA TYPE, SOURCES, AND USE

[1] IAFIS is a national fingerprint and criminal history system maintained by the FBI.

2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

The standard protocol is for the applicant to provide identifying data that will facilitate any checks the FBI conducts that are name-based. The following personal information is required to be provided by the applicant/subject of the background investigation: full name, any previous or current aliases, signature, home address, name of current employer, citizenship, Social Security number (SSN), date of birth (DOB), place of birth (POB), sex, race, height, weight, eye color, hair color, and 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 appointment to be digitally fingerprinted by Fieldprint, and validated at the time of fingerprinting.

Note: When the applicant arrives for fingerprinting, he/she must bring two valid forms of government-issued photo identification (i.e., driver's license, passport). A record is made only of the type of documents employed for identity (ID) validation; a copy of the actual documents is not made or retained by Fieldprint.

3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.

The biographical data is utilized only in those instances or aspects of the FBI records review that are name-based. A certain percentage of individuals will not be classifiable only based on their fingerprints. In those instances, a name check using IAFIS is performed with the biographical data serving as the differentiator when record hits a result that may or may not be the applicant.

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above?

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☒	☐
Social Security Number	☒	☐
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s) (non-work)	☐	☒
Email Address (non-work)	☒	☐
Employee Identification Number (EIN)	☐	☒
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☐	☒
Driver's License/State Identification Number *(*As noted above, the applicant's driver's license and passport are reviewed upon fingerprinting, but copies are not made or retained by Fieldprint.)*	☐	☒*
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☐	☒
Education Records	☐	☒
Criminal Information	☒	☐

Military Status and/or Records	☐	☒
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☒	☐
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: citizenship, sex, race, height, weight, eye color, and hair color)	☒	☐

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

a) Explain the business purpose requiring the collection of SSNs: SSN is a mandatory requirement implemented by the FBI to ensure a complete and accurate review by the CJIS.

b) Provide the legal authority which permits the collection of SSNs: 12 U.S.C. §§ 1815, 1816, 1817, 1818, 1819, 1828, 1829, 1831, and 1832; and Executive Orders 9397 and 10450, as amended.

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: SSNs are masked on the Fieldprint results web portal, but are included on the FBI Rapsheet results from CJIS. Therefore, the SSNs are visible in whole upon downloading the FBI Rapsheet results from Fieldprint. Only RMS Cyber-Fraud and Financial Crimes (CFFC) Section employees have access to the Fieldprint results site and the FBI Rapsheets. SSNs are a mandatory requirement implemented by the FBI to ensure a complete and accurate review by the CJIS.

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 ☐	1-500 ☐	501-1,000 ☐	1,001 – 2,500 ☐	2,501 – 5,000 ☐
5,001 – 7,500 ☐	7,501 – 10,000 ☒	10,001 – 50,000 ☐	50,001 – 100,000 ☐	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[2]: N/A

7. What are the sources of data (both PII *and* non-PII) for the outsourced service/project? How is the data derived?

Data Source[3] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
Financial Institution applicants submitting applications and notices to	Financial Institution applicants at the time of the investigation provide the personally identifiable information (PII) identified under question 4 to Fieldprint. Following is an explanation of	☒ Yes ☐ No

[2] If the vendor has not received work to date for this contract and "0" is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.

[3] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

the FDIC, such as applications for Federal Deposit Insurance (FDI), Notices of Acquisition of Control, applications subject to Section 19 of the FDI Act, and notices subject to Section 32 of the FDI Act.	how that data is derived. To schedule a fingerprinting appointment, the applicant visits Fieldprint's website (https://schedule.fieldprint.com), enters the appropriate FDIC code, selects a location for fingerprinting, and enters the following data: full name, email address (work or personal), previous or current aliases, signature, home address, name of current employer, citizenship, Social Security number, date of birth, place of birth, sex, race, height, weight, eye color and hair color. This information is maintained in Fieldprint's secure system for the amount of time stipulated by FDIC, after which all Fieldprint stored data is destroyed. After scheduling an appointment via Fieldprint's secure website, the applicant arrives at the designated location for fingerprinting. The applicants have their fingerprints taken by a Livescan device, which is a type of scanner that will record their fingerprint without the use of ink. Applicants must bring two valid forms of government-issued photo identification (i.e., driver's license, passport) when they arrive for fingerprinting. A record is made only of the type of documents employed for ID validation; a copy of the actual documents is not made. This record, and the PII contained therein, is retained until FDIC retrieves the FBI Criminal History Record. Response time to FDIC will be between 24 to 48 hours after fingerprinting.	
Federal Bureau of Investigation (FBI) Criminal Justice Information Services Division (CJIS)	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 then securely transmitted back to Fieldprint and held in the FDIC section of the secure Fieldprint database.	☒ Yes ☐ No

8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?

Authorized RMS personnel will retrieve the FBI results from the secure FDIC site/section of the Fieldprint system. All available records may be retrieved, or specific records pulled, using SSN, first name, or last name of applicant.

9. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

RMS's use of the Fieldprint outsourced service operates under the Financial Institution Investigative and Enforcement Records system of records (FDIC 30-64-0002).

This completes the PTA.

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
  - NOT APPLICABLE for question 3 and NO for all items in question 4; OR
  - Only Full Name in question 4.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 through 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
  - YES for Social Security Number (SSN) in question 4; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 4.

- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office (privacy@fdic.gov).

SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that will access or receive PII data as part of the outsourced service/project.

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☒	☐	When applicants/subjects of investigations 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 the FBI Integrated Automated Fingerprint Identification System (IAFIS) for processing against criminal indices. The data is transmitted to FBI 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 retrieved by FDIC. The FBI requires Fieldprint to maintain an activity log for 365 days; the log 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 Section V for information about the administrative and technical controls that Fieldprint has implemented to adequately safeguard PII in its care.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	Authorized employees within the CFFC Section of RMS receive the results of the FBI fingerprint check for use, in part, for rendering a Due Diligence determination on background investigation (BI) cases for FDIC Financial Institution applicants and for investigating current Financial Institution employees. The FBI Rapsheet results are downloaded from the Fieldprint results web portal; saved in a dedicated RMS/ CFFC Section shared drive; and attached in the Background Investigation Database System (BIDS) as a PDF document by authorized CFFC Section employees. BIDS tracks and manages BI requests for investigations of potential bank directors, officers, and principals (subjects of investigations). These data requests contain SSNs and other sensitive PII about subjects of investigations. Accordingly, BIDS requires the highest level of security possible within the FDIC and is maintained in a secured, networked environment that can be accessed only by authorized RMS personnel at Regional and Washington Office locations.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	Not applicable. As part of the services provided under this agreement, Fieldprint will not share PII with individual members of the public.
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC	☐	☒	Not applicable.

Systems/Applications			
10e. Federal, State, and/or Local Agencies	☒	☐	Authorized Fieldprint staff will securely transmit applicants' PII and digital fingerprints to the FBI 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 Section 10a 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: https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/firs-iafis.
10f. Other	☐	☒	Not applicable.

11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	☐	☒
FDIC Confidentiality Agreement (Individual)	☐	☒
Non-Disclosure Agreement (NDA)	☒	☐
Memoranda of Understanding (MOU)	☐	☒
Information Sharing Agreements (ISA)	☐	☒
Authentication Risk Assessment	☐	☒
Other Applicable Agreement(s) (*Specify*: Service Agreement)	☒	☐
If you answered NO to any item above, please provide additional information if available: RMS and DOA/Security & Emergency Preparedness Section entered into a contract with Fieldprint, Inc. in February 2018. As an "FBI-approved channeler," Fieldprint is required to adhere to the *FBI Security and Management Control Outsourcing Standards for Channelers (Outsourcing Standard)*, which stipulates adequate security and integrity controls for criminal history record information while under the control or management of Fieldprint. Refer to Section V for more information.		

SECTION IV – NOTICE AND CONSENT

12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

☐ No. Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information.

☒ Yes. 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 process, applicants are issued a written Privacy Act Statement 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 are not possible without the cooperation of the applicant.

13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?

☐ No
☒ Yes (Fieldprint collects PII via its secure online website from applicants/subjects who register to schedule a fingerprinting appointment.)

☐ Link to FDIC Privacy Policy
☐ FDIC Privacy Act Statement
☒ Contractor Privacy Policy or Statement
(http://www.fieldprint.com/FieldprintSubpage.aspx?ChannelID=163)
☐ No Privacy Policy has been posted
☐ Not applicable

SECTION V – DATA SECURITY AND ACCURACY

14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care

☒ Fieldprint, Inc. is an authorized Channeler on behalf of the Federal Bureau of Investigation (FBI) and, as such, undergoes rigorous oversight by the FBI. The *FBI Security and Management Control Outsourcing Standards for Channelers (Outsourcing Standard)*, which is discussed in more detail below, provides an overview of the FBI's requirements. As part of the FBI's Outsourcing Requirement, Fieldprint, Inc. must undergo a thorough security review by the FDIC. Such a review employs the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? ☐ NO ☒ YES

☒ The FDIC conducts background investigations (BIs) on key personnel and other applicable personnel prior to their beginning work on the contract. {Note: This important step is also performed by the FBI as part of their Channeler certification. See below for more information.}

☒ Fieldprint, Inc. is subject to periodic compliance reviews by FDIC and the FBI. Per the contract, scheduled and unannounced inspections and assessments of the Outsourced Service Provider'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.

☒ Other: The FBI conducts criminal history checks on all Fieldprint, Inc. personnel associated with the fingerprint channeling process. The FBI also requires Fieldprint, as one of its authorized Channelers, to adhere to the *FBI Security and Management Control Outsourcing Standards for Channelers (Outsourcing Standard)*, which stipulates adequate security and integrity controls for criminal history record information (CHRI) while under the control or management of Fieldprint. Adequate security as defined in the 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 *FBI Outsourcing Standard* is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy), as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. In addition, the *Outsourcing Standar*d 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.

15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date?

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

☐ The vendor/contractor works with FDIC to verify the integrity of the data [before, in conjunction with, and/or after] inputting it into the system or using it to support the project.

☐ As necessary, an [authorized user or administrator] of the [System/Project Name] checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

☒ Other: 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.

16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider.

☒ Within FDIC, the Fieldprint, Inc. 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, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this

responsibility, and the vendor has assigned an Account Executive to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data. (Refer to Section III of this Privacy Impact Assessment for more information on data access criteria.)

☒ The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

☐ None of the above. *(Explain why no FDIC staff or Outsourced Information Service Provider personnel have been designated responsibility for assuring proper use of the data.)*

SECTION VI – DATA RETENTION AND DISPOSAL

17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.

Fieldprint, Inc. maintains the record of the criminal history check on their secure website per the requirement of FDIC, which is for Fieldprint to destroy each record as soon as it has been retrieved by the FDIC. In addition, the FBI requires Fieldprint to maintain an activity log that consists of a simple chronology of who was fingerprinted and when. The log contains only of the name of the individual fingerprinted. No other PII is included.

18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.

Fieldprint, Inc. maintains the results of the search of the criminal history indices of the FBI to FDIC's specification, which is until FDIC has retrieved the data. The FBI report will be posted within an FDIC segment of their secure website. After FDIC retrieves the data, Fieldprint will then destroy the record that same day.

Per the FBI's requirements, Fieldprint must securely maintain in its system an activity log for 365 days; this log consists of a simple chronology of who was fingerprinted and when.