

PRIVACY IMPACT ASSESSMENT

SCANIT 2.86 (SCAN-IT)

November 2010

FDIC Internal System

Table of Contents

[System Overview](#)

[Personally Identifiable Information \(PII\) in SCAN-IT](#)

[Purpose & Use of Information in SCAN-IT](#)

[Sources of Information in SCAN-IT](#)

[Notice & Consent](#)

[Access to Data in SCAN-IT](#)

[Data Sharing](#)

[Data Accuracy in SCAN-IT](#)

[Data Security for SCAN-IT](#)

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

[Contact Us](#)

System Overview

The FDIC's Legal Division utilizes SCANIT 2.86 (SCAN-IT) to process electronically stored information (ESI), including file de-duplication, text extraction, tiff conversion, scanning, image optimization, optical character recognition (OCR), metadata extraction, indexing/coding, and document numbering. The Legal Division uses this application to scan, process, and export data to the FDIC's Electronic Litigation Support (ELS) application. ELS is used by Legal Division attorneys and paralegals to sort and search the data, as well as to review records for relevance to legal matters, legal privileges, and for potential redactions of personal, sensitive and/or confidential information.

The SCAN-IT application combines electronic discovery data processing, conventional paper scanning, and printing into one. It can process multiple files, find duplicates, perform OCR, and extract text and metadata. Once this application processes data, it stores metadata and the file or scanned content data in a specific "Data Directory" folder for that specific project. The Data Directory files are proprietary files used to house information for the project. These files are kept to eliminate re-processing of a project. If these files are removed from the Data Directory, all project documents or files previously scanned or processed must be re-processed before exporting to Summation.

Personally Identifiable Information (PII) in SCAN-IT

The information contained in SCAN-IT is wide-ranging in nature and may relate to any type of Corporate and/or Receivership legal matter, legal privilege, litigation discovery, FOIA request, or subpoena. Examples of the specific types of personal information that may be contained in SCAN-IT include: full name, date of birth, social security number, driver's license/state identification number, employee identification number, home address, phone numbers (e.g. phone, fax and cell), personal/corporate financial information (e.g., checking account numbers, PINs, access or security codes, passwords), banking records, or other), email addresses (non-work), employment status and/or records, and non-public financial institution data.

Data is retrieved in the Summation (ELS) system by boolean¹ search of metadata (e.g., email header fields) or searching OCR data. Typically, data is searched by author/sender, recipient, date range, document type, etc., and not by PII elements.

SCAN-IT will not derive any PII from new data that was previously non-inclusive.

Purpose & Use of Information in SCAN-IT

Use of the data in SCAN-IT is both relevant and necessary for the purpose for which the system was designed, namely to scan, process and export data to ELS for support and resolution of legal matters. This is part of the system design and is documented in FDIC's official repository, known as StarTeam.

¹ Boolean searches allow users to combine words and phrases using the words AND, OR, NOT and NEAR (otherwise known as Boolean operators) to limit, widen, or define their search.

The system is not used to monitor individuals, nor can it be used to create reports on individuals. Reports are not produced in SCAN-IT.

Sources of Information in SCAN-IT

The data in SCAN-IT is derived from electronically stored information (ESI) and paper records collected from internal FDIC systems (e.g., Enterprise Vault, and FDIC-wide email archiving solution) and individuals pursuant to litigation discovery, Freedom of Information Act (FOIA) requests, subpoenas, and other legal matters.

No federal agencies provide data directly into SCAN-IT. However, information imported or scanned into the system may be received from, for example: the Department of Justice, the Office of Comptroller of the Currency, the Federal Bureau of Investigations, the Office of Thrift Supervision, or any other law enforcement agencies or bank regulatory agencies.

No specific state or local agencies are providing data directly into SCAN-IT. However, information imported or scanned into the system may be received from a state or local law enforcement agency or bank regulatory agency.

No specific third parties will be providing data directly into SCAN-IT. However, information imported or scanned into the system may be received from parties involved in a legal matter, FDIC Outside Counsel, and other individuals or entities pertinent to the legal matter.

Notice & Consent

Individuals cannot opt out by declining to provide personal information or by consenting only to a particular use of their information in SCAN-IT. This is because the information contained in SCAN-IT is received from a variety of sources, not necessarily directly from the individual, and is necessary for processing and resolving FDIC legal matters/requests pursuant to litigation discovery, subpoenas, and/or applicable law.

Access to Data in SCAN-IT

Access to SCAN-IT is determined by the "need to know" requirements of the Privacy Act and requires the approval of the System Owner in the FDIC Legal Division. In addition, access to the application is controlled through the FDIC Identity Access Management System (IAMS) process. Guidelines established in FDIC Circular 1360.15, Access Control for Information Technology Resources, are also followed when determining access to SCAN-IT.

System administrators in FDIC's Legal Division, Information Technology Unit (ITU), Litigation Support Group have access to the system and data for purposes of processing the data and exporting it to ELS.

Also, each FDIC Regional and Area Office has a license for the SCAN-IT application, which may be utilized by authorized FDIC employees or contractors in that Office solely for scanning pertinent paper documents into the system, as requested by FDIC's Legal Division.

Contractors will have access to the system in the development environment only. Required background investigations and Confidentiality Agreements for the contractors have been developed and signed in order to permit them to work on the system.

No other agencies share or have access to the data in SCAN-IT.

Data Sharing

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

| System Name | System Description | Type of Information Processed |
|---|--|-------------------------------|
| Electronic Litigation Support (ELS) System | SCAN-IT exports data to ELS, which is used by Legal Division attorneys and paralegals to sort and search the data, as well as to review records for relevance to legal matters, legal privileges, and for the potential need to redact sensitive PII (e.g., Social Security Number) and/or confidential information. | Legal Division files/data |

Data Accuracy in SCAN-IT

Data in the system is either scanned from paper records or imported from internal FDIC systems into SCAN-IT by authorized system administrators in the Legal Division or authorized employees or contractors at FDIC Regional and Area Offices.

Information is derived primarily from FDIC ESI and paper records collected from internal FDIC systems (e.g., Enterprise Vault, an FDIC –wide email archiving solution) and individuals pursuant to litigation discovery, Freedom of Information Act (FOIA) requests, subpoenas, and other legal matters.

SCAN-IT utilizes a built-in quality control (QC) module to ensure all data has been correctly processed.

Data Security for SCAN-IT

System administrators have access to data in the system for purposes of processing and exporting data. Authorized FDIC employees or contractors at FDIC Regional and Area offices may also have access to data in the system for scanning pertinent paper documents into the system, as requested by FDIC's Legal Division.

Before access is granted to the system, authorized administrators must have the approval of the System Owner in the FDIC Legal Division. Guidelines established in

FDIC Circular 1360.15, Access Control for Information Technology Resources, are also followed when determining access to SCAN-IT.

The System Owner have overall responsibility for protecting the privacy rights of individuals whose information is contained in the system. In addition, all authorized users (i.e. system administrators) with access to the system are responsible for protecting the data. All users are required to review FDIC's Information Security Awareness Orientation training and FDIC's Privacy Act Orientation training on an annual basis, which include Rules of Behavior that focus on protecting sensitive information and sensitive personally identifiable information.

The System Owner is responsible for assuring proper use of the data. Also, it is the responsibility of every user to ensure the proper use of corporate data in accordance with FDIC Directives and the Corporate Information Security Awareness Orientation training and Privacy Act Orientation, which include Rules of Behavior that focus on protecting sensitive information and sensitive PII.

ESI processing occurs in one site. Scanning of paper documents using SCAN-IT occurs in FDIC's Regional and Area Offices. The system is used to export this ESI and scanned data to the Summation (ELS) application. The system administrators are responsible for consistent use of the system, and the same controls are used at all Offices.

FDIC has controls in place, such as virus scanning software to ensure any non-FDIC data is free from viruses and malicious code that could introduce harm in the FDIC environment.

Additionally, it is every user's responsibility to abide by FDIC data protection rules, as outlined in the Annual Security Awareness training, which all employees take and certify that they will abide by the corporation's Rules of Behavior for data protection. All authorized employees and contractors who have access to information in a Privacy Act System of Record bear some responsibility for protecting personal information covered by the Privacy Act.

System of Records Notice (SORN)

SCAN-IT does not currently operate under a SORN.

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.

