FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

CaseMap (CaseMap)

August 2013

FDIC Internal System

Table of Contents

System Overview

The FDIC Legal Division utilizes CaseMap, an evidence management system, to research, identify and organize key facts, documents, cast of characters, and issues of each case into a centralized repository for improved case management. Multiple members of a case team are able to access CaseMap at the same time. Case organization, analysis, and reporting tasks can be shared and distributed among users.

While the primary users of CaseMap are the Legal Division litigation attorneys, a small number of investigation staff from the FDIC Division of Risk Management and Supervision (RMS) and FDIC Division of Resolutions and Receiverships (DRR) also use the system. Each FDIC Regional office has a client/server version of CaseMap to allow local litigation teams to collaborate and share CaseMap data.

Personally Identifiable Information (PII) in CaseMap

Because of the wide ranging nature of FDIC legal matters resulting from bank examinations, bank closings, and enforcement actions, CaseMap has the capability to hold any and all manner of PII about current or former bank officers, employees and customers in its database. CaseMap may also retain information related to FDIC employees and contractors stemming from employment applications or personnel actions.

CaseMap stores any type of documentation that may be collected during trial preparation, including links to various types of supporting materials. As such, the documents may include employment records (for current or former bank officers or employees), bank customer records, bank contractor records, and FDIC employee or contractor personnel records with the following types of PII: full name, address, Social Security Number (SSN), maiden name, mother's maiden name, alias, and financial account information.

Purpose & Use of Information in CaseMap

CaseMap is a litigation preparation software product. Its use of the data is both relevant and necessary to the purpose for which the system is designed by indirectly relating to the Corporation's ability to execute one of its primary missions: Resolve problem and failed banks promptly and with minimal cost, by facilitating resolution of issues identified at FDIC-supervised institutions, and ensuring that potential recoveries, including claims against professionals are investigated, pursued and resolved in a fair and cost effective manner.

Sources of Information in CaseMap

Information in CaseMap is derived from a variety of internal and external sources, including:

FDIC Attorneys, Employees, and Contractors: The Legal Division litigation attorneys obtain potentially relevant electronic information stored by FDIC attorneys, employees and contractors in various locations, such as emails, desktops, laptops, network shared drives, or SharePoint sites using secure e-discovery systems[1]; the information is then uploaded to CaseMap. Relevant paper information is also obtained and scanned into CaseMap.

RMS and DRR Investigation Staff: Paper and electronic information stemming from investigations involving bank officers, employees, or customers of an open or closed bank is securely provided to Legal Division litigation attorneys for uploading to CaseMap via secured encrypted optical media, encrypted email, or by providing access to a SharePoint.

FDIC-Insured Banks/Receiverships: Open banks may provide information directly to the FDIC Legal Division during the discovery phase of litigation. Information may also come from failed bank data contained in DRR's Data Management Service (DMS) system.

FDIC Outside Counsel: Individuals at these firms who are under contract and provide support to the FDIC Legal Division securely provide paper or encrypted electronic information relevant to a legal matter to Legal Division litigation attorneys for uploading to the CaseMap system.

Federal/State/Local Agencies: At times, it is possible that other agencies such as the Department of Justice (DOJ), the Office of the Comptroller of the Currency, the Federal Bureau of Investigations (FBI), and other bank regulatory agencies may contribute paper and electronic data that is fed into CaseMap. Similarly, state law enforcement agencies or state bank regulatory agencies may also contribute paper or electronic data that is fed into CaseMap. The primary purpose of obtaining this data is to prepare for trials or resolve legal matters. The information is provided to Legal Division attorneys or other authorized FDIC staff via encrypted files or encrypted containers. The information is then uploaded to CaseMap by authorized users within the Legal Division.

External Third Parties: On occasion, external parties involved in a legal matter, such as the Outside Counsel, opposing counsel, or other stakeholders, provide paper or electronic data to FDIC Legal Division attorneys or other authorized FDIC staff via encrypted files or encrypted containers. The information is then imported into the CaseMap system by authorized administrative users in the Legal Division or other CaseMap administrative users.

[1] For further information, see the Privacy Impact Assessments for the Electronic Litigation System and Encase at www.fdic.gov.

Notice & Consent

Individuals cannot opt out from CaseMap by declining to provide personal information. The documentation stored in CaseMap is not collected directly from individuals, but obtained by FDIC litigation teams from a variety of internal and external sources, who are custodians of potentially relevant information.

Access to Data in CaseMap

The following groups of individuals have access to CaseMap:

FDIC Legal Division Attorneys and Paralegals: These individuals require access to the case files in CaseMap for the primary purpose of preparing for trials or to resolve legal matters. In addition to sorting and searching the data, FDIC attorneys and paralegals also review the records for relevance and for the potential need to redact sensitive PII (e.g., Social Security Numbers) and/or confidential information. FDIC attorneys and paralegals also physically take case data to trials or hearings using secure, FDIC-issued laptops.

FDIC Legal Information Technology Unit-Litigation Support Group (LITU-LSG): These individuals have access to CaseMap in order to assist with uploading of information to CaseMap and to conduct other system administration functions such as adding users to the system, system upgrades, and troubleshooting user reported problems. As such, they are able to view the CaseMap data.

DRR and RMS Investigation Staff: A limited member of DRR and RMS Staff have access to CaseMap data pertaining to investigations that they actively work on involving bank officers, employees, or customers of open or closed banks.

FDIC Outside Counsel: Individuals at these firms have indirect access to CaseMap data, in order to provide support to Legal Division attorneys on various legal Matters. Data is provided to Outside Counsel via secure mechanisms by authorized FDIC Legal Division attorneys, paralegals or LITU-LSG staff.

FDIC Division of Information Technology (DIT) staff: Employees and contractors in the DIT Infrastructure Services Branch provide network access and system troubleshooting support. They do not need nor have access to CaseMap data to perform these duties.

All authorized users (i.e. system administrators) with access to the system are responsible for protecting the data. All users are required to complete FDIC's Information Security and Privacy Awareness Training Course on an annual basis, which include Rules of Behavior that focus on protecting sensitive information and sensitive personally identifiable information. Only authorized users have access to the data stored in CaseMap, including reports.

Additionally, users will not have access to all of the data in the system. Rather, they only access data pertaining to cases within their specific FDIC region. Also, the CaseMap Administrator has the ability to restrict authorized users within a specific region to individual cases.

Access is determined on a "need to know" basis and requires the approval of the CaseMap Program Manager/System Owner in the FDIC' Legal Division.

Data Sharing

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

No other systems currently share or have access to the data in CaseMap.

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

Data Accuracy in CaseMap

FDIC Legal Division attorneys and paralegals using CaseMap enter or import data into the system that are deemed relevant to specific cases. Data received from other sources are scanned and uploaded from pre-existing documents into the CaseMap system by LITU-LSG system administrators for access by Legal Division attorneys and paralegals. Data is manually reviewed for relevance, accuracy, and privileges.

Data Security for CaseMap

CaseMap system security is provided on two levels: network security and application (standard) security. Network security is provided by the group level permissions for the folders and their subfolders and defines which user groups have which folder permissions. At the application level, security is provided through the Administrator Console, an internal device through which the system administrator defines groups, assigns permissions to each group, and adds user IDs to each group and case.

System of Records Notice (SORN)

CaseMap does not currently operate as a Privacy Act Systems of Records. Data can only be retrieved (by an authorized user with permission and access to the system) by case, bank name, or other non-PII identifier.

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.