

PRIVACY IMPACT ASSESSMENT

Claims Administration System (CAS)

November 2009

FDIC Internal System

Table of Contents

[System Overview](#)

[Personally Identifiable Information \(PII\) in CAS](#)

[Purpose & Use of Information in CAS](#)

[Sources of Information in CAS](#)

[Notice & Consent](#)

[Access to Data in CAS](#)

[Data Sharing](#)

[Data Accuracy in CAS](#)

[Data Security for CAS](#)

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

[Contact Us](#)

System Overview

The FDIC insures all deposit accounts, including checking and savings accounts, money market deposit accounts and certificates of deposit. During the failure of a FDIC-insured financial institution, the FDIC is responsible for analyzing and processing claims from insured depositors, i.e., individual bank customers, brokers (acting as agents for other depositors), businesses, and governments. Generally referred to as "depositors," these are individuals or entities that are entitled to receive payments from the FDIC, acting in its receivership capacity. The larger the size of the insured institution, the greater the demand that is placed on FDIC staff and resources to process claims in a timely and accurate manner.

Throughout the bank closing process, the FDIC's Division of Resolutions and Receiverships (DRR) has the primary responsibility for processing depositor claims. The purpose of the Claims Administration System (CAS) is to enhance FDIC's ability to process claims in a timely manner, regardless of the insured institution size and complexity. CAS is used to determine deposit insurance amounts and to process deposit insurance claims when a financial institution fails.

CAS supports the downloading of datasets containing depositor information from both large and small financial institutions in order to decrease the amount of manual work done primarily by DRR Claims Staff (including Claims Agents) and DRR Business Information Systems (BIS) Staff, as well as work performed by other DRR staff involved in the closing process.

Personally Identifiable Information (PII) in CAS

CAS contains both PII and non-PII about depositors. The data is obtained directly from the institution by the DRR BIS Staff, as part of an overall transfer of the Customer Information File (CIF) to the FDIC during the bank closing process. BIS Staff extracts the following data elements and prepares the data for use by CAS and authorized DRR staff:

- Full Name of Bank Customer (including primary account holder, trustees or beneficiaries)
- Date of Birth
- Social Security Number (SSN) or Taxpayer Identification Number
- Home Address
- Phone Numbers (non-work)
- Financial Information (e.g., checking and savings account numbers and balances)
- Type of account (e.g., single/joint account; revocable trust account; corporate, partnership and unincorporated association account; irrevocable trust account; employee benefit plan account; or government account)

Purpose & Use of Information in CAS

The use of the personal information is relevant and necessary for the critical business functions supported by CAS at the time of a bank closing. Personal information is necessary for identification of depositors, making insurance determinations, and

ensuring the payout of claims. This use is documented in the system Design Document and the User's Manual. The System documentation is maintained in FDIC's official repository, known as StarTeam.

Sources of Information in CAS

The PII and other sensitive bank depositor data contained in CAS is obtained from three primary sources:

Failing/Failed Financial Institution: Using secure methodologies, the DRR BIS Staff obtains the Customer Information File from the failing or failed institution. The BIS Staff then extracts/prepares the required depositor data elements for uploading to CAS. The BIS Staff is responsible for ensuring the completeness of the data downloads, prior to use by CAS.

Individual Bank Depositor: On occasion, the FDIC Claims Staff requires additional support data or documentation from depositors to make insurance determinations. This occurs when there are questions about the ownership status of the account. This collection typically occurs during an in person meeting. The required information is entered into the CAS system by authorized Claims Staff.

FDIC Receivership Liability System (RLS): Upon its retirement, data contained in RLS was migrated to CAS.

Notice & Consent

The information in CAS is not obtained by the FDIC directly from individuals, but instead through a download of the data from the failed financial institution during the closing process; therefore there is no opt-out option for individuals. In some instances, DRR Claims Agents may require further information from an individual to resolve a claim. When additional data is necessary to prove a claim, there is no opt-out option for individuals wishing to receive payment.

Access to Data in CAS

The primary users of CAS are authorized FDIC employees and contractors within FDIC's Division of Resolutions and Receiverships (DRR). DRR uses CAS to support their claims administration process as part of the resolution of a failed financial institution. Within DRR, the following groups require the use of CAS:

- **Claims Staff/Claims Agents** – Analyze and determine depositor claims. Additionally, they prepare related internal management reports concerning insured and uninsured depositors.
- **Business Information Systems (BIS)** – Prepare depositor data obtained from the failing/failed bank for use by CAS.

- **Customer Service** – Respond to depositor calls about their claim status or to schedule an appointment with a Claims Agent to further resolve questions about a claim.
- **Investigations** – Support professional liability claims resulting from fraud/negligence on the part of directors, officers, attorneys, accountants, brokers and others.
- **Accounting** – Process the payout of depositor claims and other accounting matters.
- **Contractors** – Provide support to the Claims and BIS Staff due to the high workload stemming from increased bank closings.

Other authorized internal FDIC users will be in the Division of Information Technology (DIT), which is responsible for providing technical support during the construction of the system, confirming adherence to FDIC policies and standards (e.g., security and privacy), and providing system administration and maintenance support upon completion. Due to the high number of bank closings, DRR may ask staff from other FDIC divisions, particularly those who have obtained FDIC Claims Certifications, to assist with closing activities. This may temporarily increase the number of authorized CAS users, during the period known as "closing weekend." The closing weekend is when FDIC takes over the failed institution, after having been appointed as the receiver by the bank's chartering authority. The user's access will be removed or deactivated in CAS once they return to their regular duty station, soon after the closing weekend.

Data Sharing

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

System Name	System Description	Type of Information Processed
Dividend Processing System (DPS)	DPS is an existing DRR system used to generate payments, including payout checks, to insured depositors during bank closings. CAS sends and receives payout information to DPS containing sensitive PII related to bank account holders.	Full Name, Social Security Number or Taxpayer Identification Number, Home Address Financial Information (checking or savings account numbers and balances)
Non Deposit Claims System (NDC)	NDC is a DRR system developed to support the processing of non-depositor claims (also referred to as creditor or general trade creditor claims) filed by individuals or entities against the FDIC receivership.	Date of Bank Closing, First Notice Publication Date (i.e., date when notice of bank closing is published by FDIC in the local newspaper(s)).
Division of Resolutions and Receiverships Internet Publications (DRRIP)	DRRIP is an external FDIC web site that allows customers of failed banks to determine whether their accounts are fully insured or if they need to contact FDIC.	Failed Bank Name, Bank Customer Account Number, Status of insured or uninsured funds

Data Accuracy in CAS

Data entry screens and load modules managed by the DRR BIS Staff include edit checks, to ensure that business rules and data relationships are maintained. Data validation has been incorporated within the application (front-end) and the database (back-end), to ensure data is entered in the required format. There are validations at the data field level (e.g., monetary fields must be numeric). There are calculated fields to avoid manual entry errors. DRR BIS Staff also analyze the data downloads for reliability and prepare the data for use by the various FDIC systems and business processes that support the overall closing effort, including CAS.

Data Security for CAS

All authorized users who have access to the CAS data must have the approval of their Manager/Supervisor and the DRR CAS Program Manager/Data Owner before access is granted to the system. Additionally, CAS' functional security limits a user's access to specific functions and regulates a user's ability to update data for a specific function. All access granted is determined on a "need to know" basis. Guidelines established in the Corporation's Access Control Policies and Procedures document are also followed. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

System of Records Notice (SORN)

CAS operates under the FDIC Privacy Act SORN 30-64-0013, *Insured Financial Institution Liquidation 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.

