FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Investigations Restitution Tracking Utility (IRTU)

December 2014

FDIC Internal System

Table of Contents

System Overview

When a financial institution fails, and the Federal Deposit Insurance Corporation (FDIC) is appointed as receiver,[1] one of the FDIC's primary tasks is to dispose of the failed bank's loans and assets in a manner that maximizes their value. Occasionally, when a financial institution fails and the FDIC takes over as receiver, the FDIC must engage in legal remedies to recoup funds as a result of faulty or illegal activity against the failed bank. If the FDIC is successful in their pursuit of recovery, the Federal or State court will issue an Order of Restitution naming the FDIC as an injured party. This Order of Restitution provides the FDIC with the legal authority to collect the amount of the court ordered restitution from the parties listed in the court order.

Investigations Restitution Tracking is the process by which the FDIC Division of Resolutions and Receiverships (DRR) tracks collection processes resulting from Restitution Orders handed down by the court systems. This process includes documenting collection strategies, allowing Account Officers to enter and store activity comments, track incarceration status of defendants, annotate event driven ticklers for Account Officers and tracking of financial payment information related to the restitution order generated asset.

The Investigations Resolution Tracking Utility (IRTU) application is used by FDIC's DRR Investigations Section to collect restitution-related asset and case tracking data from two FDIC sources most commonly used for the collection process: (1) DRR Locator and Reporting System (DOLLARS), which is the FDIC's primary restitution case tracking and strategy annotation application, and (2) the Communication, Capability, Challenge and Control system (4C), which is the FDIC's primary application for Asset, Borrower, and Associated Party data for failed institutions. IRTU gathers data from these two FDIC applications and presents the FDIC/DRR Account Officer via a custom user interface with a comprehensive centralized location for viewing all case-related data. Additionally, IRTU provides a functionality that is not currently supported by 4C or DOLLARS, including the capability to house and update various case related contact information for Assistant United States Attorneys (AUSA), Probation/Parole Officers and other applicable parties associated with restitution cases.

Personally Identifiable Information (PII) in IRTU

Many of the individuals involved in restitution collection efforts are also criminally liable for their activities. As such, IRTU collects and maintains contact information for a variety of parties associated with restitution cases such as: Borrower (Defendant), Participant (Co-Defendant), Assistant United States Attorneys (AUSA), Primary Investigator, Clerk of the Court, Probation/Parole Officer Borrower Name. Data collected pertaining to the Borrower (Defendant) includes the borrower's name,

[1] A receiver steps into the shoes of a failed financial institution with the goal of liquidating the entity. Federal law grants the FDIC the responsibility to manage the resolution of failed financial institutions. The FDIC as the receiver has similar powers and responsibilities as a bankruptcy trustee. The FDIC can collect all obligations and money due to the failed institution and liquidate its assets and property. The funds generated are used to pay the creditors of the failed institution. Although many of the concepts central to the operation of an FDIC receivership are similar to those of the bankruptcy process, there are critical differences between bankruptcy and receivership law.

home address, email address, telephone number, fax number, restitution order date, statute of limitations date, loan original balance, asset net balance, docket number, judicial district, loan maturity date, and prison release date (if applicable). Data collected pertaining to the Participant (Co-Defendant) includes name, home address, and prison release date (if applicable). IRTU contains names, work email addresses, work telephone numbers, and work fax numbers of Assistant US Attorneys, Clerks of the court, and Probation/Parole Officers. The system also contains data pertaining to FDIC personnel, which includes: Managing Account Officer (AO) name, Marketing Account Officer Name, DRR Investigator Name, Investigator's Supervisor/Manager name, and name the FDIC Attorney assigned to the case.

In addition to the above PII, IRTU contains comments which may include contextually sensitive information about the case or the defendants. IRTU also contains a variety of non-PII, including but not limited to: failed and assuming institution data, asset balance data, criminal restitution order data (e.g., status, court docket, date ordered, date booked, etc.), fund type, asset type, etc.

Purpose & Use of Information in IRTU

FDIC/DRR Account Officers, working with attorneys who represent either the FDIC or the jurisdiction bringing legal charges, are tasked with the effort of collecting court awarded damages owed to the FDIC as a result of a successful prosecution against one or more accused parties. Previously, the Account Officer accomplished this task through utilizing the following FDIC systems: DOLLARS, 4C, New Financial Environment (NFE), and Control Totals Module (CTM). IRTU simplifies and streamlines the AO's business process by providing a single location for pertinent case-related information and details required to manage the collection effort, along with consolidated reporting on the collection effort. All data maintained in IRTU is necessary to support and manage this Investigations Restitution Order collection and tracking process.

Sources of Information in IRTU

The originating sources of data in the IRTU system include: the FDIC Communication, Capability, Challenge and Control (4C) system and the DRR Locator and Reporting System (DOLLARS). Data imported from 4C includes investigation asset detail, asset participant information, and asset financial transaction data. Data imported from DOLLARS consists of investigations asset data to include restitution collection case comments and collection strategy directives.

Data is extracted from the DOLLARS system and delivered to an interim staging area in the FDIC's Enterprise Data Warehouse (EDW). Once it resides in the EDW, it is pulled directly by the IRTU application for consumption into the core database tables. Data extracted from 4C is delivered via an Extract, Transform and Load (ETL) process directly to staging tables in the IRTU database on an interim basis. In 2015, the 4C data mart will have been migrated into the EDW and the ETL process will be retired; the required 4C data will be pulled directly via a database view from the data mart.

In addition to the above data sources, authorized FDIC/DRR Investigations staff manually enters information into the IRTU application, such as contact information for the AUSA, Primary Investigator, Clerk of the Court, and Probation/Parole Officer for each case. All data entered by FDIC staff is based on Court-Issued Orders of Restitution naming FDIC as an injured party. This data is obtained by FDIC personnel from public records of the state and federal court systems.

Notice & Consent

Individuals do not have the opportunity to "opt out" of providing their information for inclusion in IRTU. The data is obtained directly from other FDIC systems or entered manually by authorized FDIC/DRR staff based on data obtained from public records and through FDIC internal legal representatives. The data is necessary to support and manage the FDIC's Investigations Restitution Order collection and tracking process. Therefore, no opt-out is provided.

Access to Data in IRTU

FDIC/DRR Investigations staff requires access to IRTU in order to track collection efforts based on Court-Issued Orders of Restitution naming the FDIC as an injured party. Within FDIC's DRR Investigations Section, a limited number of authorized staff will have access to IRTU, including approximately five (5) Investigations Account Officers, three (3) Investigations Managers, 3 Investigations Technicians, and 3 Administrators. All users who have access to the data must have the approval of their Manager/Supervisor and the Program Manager/Data Owner of the requested capability in order to be granted access. Additionally, IRTU's functional security limits a user's access to specific data and restricts the user's ability to update data based on the specific functions assigned to his/her level of access. All access granted is determined on a "need to know" basis. Guidelines established in the Corporation's Access Control policies and procedures are also followed. Controls are documented in the official FDIC system documentation. A user's access is requested and tracked via the Corporation's access control tracking system [Identity Access Management System (IAMS)].

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 in IRTU

A data quality report is generated when there are discrepancies between 4C and DOLLARS key data elements. Additionally, the Program Managers/Data Owners for IRTU and DRR Information Security Manager serve as the source of information for data definition and data protection requirements.

Data Security for IRTU

Access levels and permission levels have been established, and access is granted only to those persons who have “a need to know” the information contained in the system in order to carry out their official job duties. In accordance with OMB Circular A-123, and A-130, Appendix III, the IRTU system has controls in place to prevent unauthorized access to the data in the system. Security measures and controls consist of, for example: user identification and authentication, database permissions and software controls.

Additionally, IRTU’s functional security classifies each user into one of the established business roles (i.e., Account Officers, Technicians, Managers, and Administrators). As a result, the authority granted to a user’s access role governs the user’s ability to access or manipulate information. The user’s Manager or the Program Manager/Data Owner determines the business role a user will be assigned based on his/her job function or purpose for accessing the system. When a user logs into IRTU, he/she can only view and or edit those fields dictated by his/her respective business role.

An audit trail process captures data manipulations (i.e., insert, update or delete), identifying who performed the data manipulation and when the data manipulation was performed. All users of the IRTU system must complete DRR’s Security Awareness Training and the mandatory Corporate Information Security and Privacy Awareness training module. This training is required annually for all FDIC employees and contractors with network access. It includes the Rules of Behavior and has specific information regarding compromise and the prevention of misuse of data.

In addition, it is every IRTU user’s responsibility to assure proper use of the data they access in the system. All FDIC users of the IRTU system must complete and abide by the DRR Security and Privacy Awareness Course which encompasses all DRR applications and network resources. In addition, all FDIC network users are required to complete the Corporation’s annual Information Security and Privacy Awareness Training, which includes the Rules of Behavior to which all users must adhere. This training also states specifically the rules for protecting and preventing the compromise and misuse of sensitive information and PII.

System of Records Notice (SORN)

IRTU 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.