FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Enforcement Decisions and Orders (EDO 2.0)

December 2011

FDIC Internal System

Table of Contents

System Overview

The FDIC Legal Division uses the Enforcement Decisions and Orders (EDO) system to track and publish formal enforcement actions[1] against banks that are regulated by the FDIC or against their institution-affiliated parties (IAPs) (e.g. bank officers and employees). The determination to pursue an enforcement action against a bank or its officer/employee is made by FDIC's Division of Risk Management Supervision (RMS), and/or by FDIC's Division of Depositor and Consumer Protection (DCP), in conjunction with the Legal Division.

Currently, the EDO system electronically routes EDO documents between authorized users within the Legal Division who are required to review and approve the EDO documents before they are published on FDIC's public website (www.fdic.gov/bank/individual/enforcement/). EDO 2.0 involves the addition of a third-party product, BizFlow, as the workflow engine. The workflow is designed to capture EDO data (via user input screens) and documents for automated routing between authorized users within the Legal Division for review and approval prior to publishing to FDIC's public website. During this phase, the EDO data is considered sensitive and will be stored in an Oracle database within the secure FDIC network.

Once the data is approved for release, the EDO 2.0 system will automatically publish decisions, orders, and accompanying press releases to the EDO's public-facing website. EDO 2.0 also enhances the search engine used by the public by providing for multiple search criteria against metadata in the EDO records, allowing queried results to display matching records and their associated EDO documents. The query results will also indicate whether the original orders have been modified or terminated. The published data is considered non-sensitive and will be stored in a SQL database on FDIC.gov.[2]

Personally Identifiable Information (PII) in EDO 2.0

The EDO system contains information on the following entities and individuals:

- FDIC-insured state chartered banks that are not members of the Federal Reserve System;
- FDIC-insured branches of foreign banks; and
- Officers, directors, employees, controlling shareholders, agents and certain other categories of individuals (institution-affiliated parties) associated with such institutions.

The EDO database includes the following data fields: category, year, page, para, docket, new docket, action code, institution/bank, party, order, action, city, state, effective, and term date. The only data field that contains personally identifiable

[1] Types of enforcement actions include: consent orders, removal and prohibition orders, prompt corrective actions, and cease and desist orders. Publication of this information is required by 12 U.S.C. § 1818 (u). Additional information about enforcement action activities may be found in the Privacy Impact Assessment for the FDIC VISION system (Formal and Informal Action Tracking module).

[2] Enforcement orders are announced to the public in a monthly press release listing all final enforcement orders issued by the FDIC during the previous month. Printed copies of the enforcement orders are available in the Public Information Center, 3501 North Fairfax Drive, Room E-1002, Arlington, VA 22226. Telephone (703) 562-2200 or (877) ASK-FDIC, at the time the press release is issued.

information (PII) is "party" or "order," which includes the full name of the individual bank officer or employee named in the enforcement action. The information is maintained in the internal Oracle EDO database while the FDIC Legal Division reviews, tracks, and provides approval for the enforcement actions. While maintained in this internal Oracle EDO database and prior to publishing of the enforcement actions on the EDO web page, the name of the individual or financial institution combined with the enforcement action information is considered sensitive PII. Once the content is published to the online database, it becomes publicly available information.

EDO users have numerous retrieval options for the data prior to it being published to the public website. EDO users primarily retrieve data by party or order name, which may be an individual or financial institution's full name who is subject to the enforcement action.

Once the data has been approved and published to the EDO public web site on FDIC.gov, the public user will be able to run a search for decisions and orders based on an individual's name.

EDO does not collect any information on individuals using the EDO search engine on FDIC.gov.

Purpose & Use of Information in EDO

The use of this data is both relevant and necessary to the purpose for which the EDO was designed, specifically to process, track and publish FDIC Enforcement Decisions and Orders. This functionality is part of the system design and is documented in FDIC's official repository known as StarTeam.

EDO allows users to produce five reports. All of the reports may contain an individual's name (bank and title) when available and may be associated with an Enforcement Decision or Order. All reports are accessible through the EDO application only. All EDO users will have the capability of running/viewing all reports within the application, and to save or print them out.

Sources of Information in EDO 2.0

Enforcement action data containing PII is obtained from authorized individuals in FDIC's Division of Risk Management (RMS), Division of Depositor and Consumer Protection (DCP), and the Legal Division. The data is then manually uploaded to the EDO database by authorized users of the Legal Division.

Notice & Consent

Per the FDIC's statutory authority, it may pursue enforcement actions for violations of laws, rules, or regulations, unsafe or unsound banking practices, breaches of fiduciary duty, and violations of final orders, conditions imposed in writing or written

agreements. As such, individuals cannot "opt-out" by declining to provide personal information or by consenting only to a particular use.

Access to Data in EDO 2.0

Access to EDO 2.0 is determined by the "need to know" requirements of the Privacy Act and requires the approval of the Legal Division EDO Program Manager. All users must have the approval of their Manager/Supervisor and the Legal Division EDO Program Manager before access is granted to the system. Not all users will have access to all data in EDO. Only authorized users have access to the data stored in the system, including reports. Certain types of authorized user roles will be granted for read-only access; and only specific users will be granted permission to create, update, delete, or route the EDO data.

Authorized internal users in the following groups have access to data in the EDO system. Also, authorized users may only view and edit documents depending on their restricted privileges:

1. **FDIC Legal Division Staff:** including Legal Specialists and Legal Reviewers from the Legal Enforcement Section to process and approve EDO data (e.g. Orders, Press Releases and Administrative Hearing data) for public release;
2. **FDIC Office of Public Affairs (OPA) Staff:** including Public Affairs Specialists and Web Content staff to create the Press Release and publish approved EDO documents on FDIC.gov;
3. **EDO System Administrator:** to monitor and manage the system and user access; and
4. **FDIC Division of Information Technology (DIT) staff and contractors:** including Database Administrators, who have full access to the internal EDO database; BizFlow Administrators, who will have full access to the BizFlow data in both databases; and System Developers, who will not have access to the EDO production data prior to it being published to the public website.

Contractors employed by FDIC's Division of Information Technology have been integral in the design and construction of the EDO system and provide technical and maintenance system support of the system, but do not have access to the production environment.

Each contractor who has access to EDO and/or source data is required to complete the FDIC's Privacy Act Awareness Orientation and Information Security Awareness Training, which includes the Corporate Rules of Behavior. They are also required to sign an FDIC Contractor Confidentiality and Non-Disclosure Agreement.

Data Sharing

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

No other systems share or have access to the data in EDO 2.0.

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

Data Accuracy in EDO 2.0

Data will be checked for completeness by visual inspection by authorized EDO users. The data is then manually entered into the EDO system. The EDO system will alert the user if certain required information is missing.

Data Security for EDO 2.0

The EDO system has controls in place to prevent the misuse of the data by those having access to the data. Such security measures and controls consist of: passwords, user identification, IP addresses, database permissions, and access controls.

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.

Additionally, EDO (through the BizFlow product) includes audit records that log user ID and time(s) when data is created, updated or routed to another user group.

While the Legal Division EDO Program Manager ultimately is responsible, all users of the system bear responsibility for protecting the privacy rights of individuals, whose personal information is in the system. Policies and procedures for responsibility and accountability are included in the FDIC's Privacy Act Awareness Training, which includes the Corporate Rules of Behavior. All users of FDIC systems must annually certify that they agree to abide by the Rules of Behavior to retain access to FDIC systems.

The EDO Program Manager is responsible for ensuring that sufficient safeguards and controls are in place to avoid the unauthorized or unintended release of personal data, while individual EDO users are responsible and accountable for assuring the proper collection and use of the data. The Program Manager also has overall responsibility for the EDO application and is accountable for establishing the criteria,

procedures, controls, and responsibilities to prevent a compromise of the integrity of the data being collected.

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)

EDO 2.0 operates under the FDIC Privacy Act System of Records Notice (SORN) 30-64-002, *Financial Institution Investigative and Enforcement 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.