Table of Contents

System Overview
Personally Identifiable Information (PII) - FCX
Purpose & Use of Information - FCX
Sources of Information - FCX
Notice & Consent
Access to Data - FCX
Data Sharing
Data Accuracy - FCX
Data Security - FCX
System of Records Notice (SORN)
Contact Us
System Overview
The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and public confidence in the nation's financial system. FDIC preserves and promotes public confidence in the U.S. financial system by:

- insuring deposits in banks and thrift institutions for at least $250,000;
- examining and supervising financial institutions for safety and soundness and consumer protection;
- managing receiverships; and
- resolving failing institutions to limit the impact of the failure of a bank or thrift on insured depositors and the economy.

To fulfill its mission, and to comply with the Government Paperwork Elimination Act of 1998 (GPEA), the FDIC developed the FDICconnect (FCX) system to provide a secure channel for financial institutions, state banking authorities and other organizations to efficiently and effectively conduct business with the FDIC to support FDIC business functions.

Multiple divisions and offices within FDIC utilize the data contained in FCX, accessing only data which is within their scope of authority to accomplish their respective business functions. The FDIC Divisions and Offices currently utilizing FCX, include:

- Division of Consumer Protection (DCP)
- Division of Insurance and Research (DIR)
- Division of Information Technology (DIT)
- Division of Finance (DOF)
- Division of Receiverships and Resolutions (DRR)
- Legal Division
- Office of Complex Financial Institutions (OCFI)
- Office of the Ombudsman (OO)

Personally Identifiable Information (PII) - FCX
The purpose and functionality of FCX is to provide a secured conduit for exchanging large files. As such, FCX is not specifically designed to collect, use or maintain sensitive PII. However, FCX has the capability to retain transmitted files indefinitely for retrieval by authorized FDIC users until the sessions reach their expiration date. FCX has both a “Session Close Date” and a “Session End Date.” The Session End Date means that the session is no longer available to the bank or company; however, the information remains available to FDIC for 17 days. The end of day 17 marks the Session Close Date. Sessions and files are purged 30 days after the Session Close Date. These files may contain a wide variety of sensitive data and PII, depending on what type of data is transmitted by the various Divisions/Offices and authorized external organizations that utilize FCX in their support of FDIC’s mission. Types of sensitive data and PII which could potentially be included are: full name, date of birth, place of birth, Social Security number, employment information, mother's maiden name, certificates, medical information, home address, phone number, email address, employee identification number, financial information,
driver’s license, vehicle identifier, legal documents, education records, criminal information, military status, and photographic identifier.

**Purpose & Use of Information - FCX**
The FDIC developed FCX to facilitate secure electronic communication with external parties, including FDIC-insured financial institutions, state banking departments, and other federal agencies. Multiple divisions and offices within FDIC utilize FCX to support their respective business functions.

**Sources of Information in FCX**
FCX receives information from financial institutions, FDIC systems, and authorized federal and state agencies, as shown below:

<table>
<thead>
<tr>
<th>Data Source</th>
<th>Description of Information Provided by Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structure Information Management System (SIMS)</td>
<td>Financial Institution lookup and status data</td>
</tr>
<tr>
<td>Assessment Information Management System (AIMS)</td>
<td>Assessment invoices and other correspondence</td>
</tr>
<tr>
<td>Specialized Tracking and Reporting System (STARS)</td>
<td>Consumer complaint information</td>
</tr>
<tr>
<td>Virtual Supervisory Information on the Net (ViSION)</td>
<td>Application status</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>Bank information and requests; and bank customer information</td>
</tr>
<tr>
<td>State Banking Regulators</td>
<td>Information relating to bank examinations, which may include PII of bank employees and/or bank customers</td>
</tr>
<tr>
<td>Federal Reserve</td>
<td>Information relating to bank examinations, which may include PII of bank employees and/or bank customers</td>
</tr>
<tr>
<td>Office of the Comptroller of the Currency (OCC)</td>
<td>Information relating to bank examinations, which may include PII of bank employees and/or bank customers</td>
</tr>
<tr>
<td>FDIC Ombudsman</td>
<td>Complaint resolutions</td>
</tr>
<tr>
<td>Bank Customer</td>
<td>Information relating to bank customer complaints, which may include name and specifics concerning bank practices or bank employees</td>
</tr>
<tr>
<td>Bidders</td>
<td>Expressions of Interest</td>
</tr>
</tbody>
</table>
Notice & Consent

Individuals may not opt out of providing their personal information to FCX. Data is not collected directly from individuals. Rather, data is provided by the financial and state banking entities who conduct business with the FDIC. FDIC requires this data to fulfill its mission and mandated obligations as regulator, receiver and insurer of financial institutions; therefore, no opt-out is provided.

Access to Data – FCX

Access 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 based on their official job duties/responsibilities. Access requests for FDIC users are controlled and tracked via the FDIC’s Identity Access Management System (IAMS) process. All users who have access to the data must have the approval of their Manager/Supervisor, and the Program Manager/Data Owner responsible for the data to which access is granted.

FCX is used by multiple Divisions and Offices of the FDIC to fulfill various agency-mission goals. In general, internal users of the system include: authorized FDIC personnel staff, supervisory personnel, management officials, system administrators, and other employees of the FDIC who have an authorized “need to know” the information contained in system to carry out their duties. In certain instances, contractors performing work on the FDIC’s behalf may have access to the records in the system.

Externally, the FCX system provides a secure channel for financial institutions, state banking authorities and other organizations to efficiently and effectively conduct business with the FDIC.

External users: The FCX business center is the secure internet channel for FDIC-insured institutions to conduct business and exchange information with the FDIC. To initiate the application process, the insured institution must apply to FDIC to participate and designate someone as a Coordinator for their institution. The Coordinator must register and become “associated” with their institution. Coordinators approved by FDIC can then approve others to be authorized to perform transactions. Coordinators must complete a coordinator registration form, available strictly from the FCX Helpdesk; and complete their online registration through FDICconnect.gov. Coordinators authorize users; all authorized users must complete the online registration.

The portal displays a Security notice to individuals accessing the site and provides a link to the FDIC Privacy Policy Statement.

Internal users: FDIC business divisions are responsible for establishing and promulgating the procedures for controlling access to the data transmitted via FCX. The FCX platform provides controls for auditing who accesses information via FCX. Access to the data is restricted to a “need to know” basis. An FCX user’s profile is based on the user’s job requirements, managerial decisions, and dependent on the purpose for which access to the data is needed. Access requires management
approval, and is facilitated using the FDIC’s Identity Access Management System (IAMS).

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

<table>
<thead>
<tr>
<th>System Name</th>
<th>System Description</th>
<th>Type of Information Processed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment Information Management System (AIMS)</td>
<td>AIMS is a web-based application that performs calculation and billing as well as supports the collection of assessments for FDIC-insured institutions.</td>
<td>Assessment points of contact and ACH information supplied by bankers that is delivered to AIMS.</td>
</tr>
<tr>
<td>Specialized Tracking and Reporting System (STARS)</td>
<td>STARS is a customized tracking and workflow system designed to track incoming correspondence and telephone calls from consumers and bankers that are not examination related.</td>
<td>Responsive documents and information supplied by bankers to consumer complaints that are delivered to STARS.</td>
</tr>
<tr>
<td>Virtual Supervisory Information on the Net (ViSION)</td>
<td>ViSION is a web-based system used primarily to assess risks to the deposit insurance fund associated with the operations of insured depository institutions and their affiliates and servicers, such as data processing servicers.</td>
<td>Application data provided by bankers that is delivered to ViSION.</td>
</tr>
<tr>
<td>Overarching Automation System (OASIS)</td>
<td>OASIS is used to track all the activities related to the resolution of a failing institution from the time of notification to the date of close.</td>
<td>Contact information and acquisition preference data supplied by banker that is delivered to OASIS.</td>
</tr>
</tbody>
</table>

Data Accuracy - FCX
Each Division and its respective users are responsible for verifying the accuracy, timeliness, and completeness of data transferred through FCX.
Data Security – FCX
FCX operates under the FDIC’s common controls, which are intended to produce the policies and procedures required for the effective implementation of selected security controls and control enhancements as identified in the security planning family. The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy.

Additionally, FDIC conducts continuous monitoring of security controls using automated support tools, facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well-executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system.

Rules of Behavior are defined for FCX. New users are required to accept the rules as part of the user provisioning process by establishing and making readily available to all information system users both (a) the rules that describe their responsibilities and expected behavior with regard to information and information system usage and (b) Special Publication 800-53 Recommended Security Controls for Federal Information Systems and Organizations. In addition, before the FDIC authorizes access to FCX, the user must provide a signed acknowledgment indicating that they have read, understand, and agree to abide by the rules of behavior.

The FCX platform is regularly scanned to identify security vulnerabilities. A combination of application access control, database access control, and file system permissions are used to protect data from unauthorized use.

System of Records Notice (SORN)
FCX does not operate as a System of Record.

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.