



Privacy Impact Assessment of the Fair Lending Tool

Program or application name.

Fair Lending Tool

System Owner.

Board of Governors of the Federal Reserve System's Division of Consumer and Community Affairs

Contact information.

System Owner: Timothy Burniston, Senior Associate Director
Organization: Division of Consumer and Community Affairs
Address: 20th and C Streets, N.W.
Washington, DC 20551
Telephone: (202) 452-3488

Program Manager: Cliff Follweiler
Organization: Division of Consumer and Community Affairs
Address: 20th and C Streets, N.W.
Washington, DC 20551
Telephone: (202) 736-5660

IT System Manager: Mari Murphy
Organization: Division of Information Technology
Address: 20th and C Streets, N.W.
Washington, DC 20551
Telephone: (202) 872-4938

Description of the IT system.

The Fair Lending Tool (FLT) is used to analyze lending and demographic data gathered from regulated financial institutions. FLT is used by the Consumer Compliance Supervision (CCS) function throughout the Federal Reserve System (Federal Reserve). Federal Reserve staff use FLT on all consumer compliance examinations of financial institutions for the purpose of Community Reinvestment Act (CRA) and fair lending data analysis and compliance with applicable laws and regulations. Federal Reserve staff also use FLT to analyze Home Mortgage Disclosure Act (HMDA) data submitted to the Federal Financial Institutions Examination Council (FFIEC) by financial institutions, who are required under the Board's Regulation C to submit their HMDA lending data to the Federal Reserve on an annual basis. Examiners can also analyze institution specific CRA data which includes small business and small farm data. This submitted data is used by the FFIEC regulators, including the Board of Governors of the Federal Reserve System (Board), to assess financial institutions' compliance with the Board's HMDA and CRA regulations and the Board's overall HMDA data analysis. Finally, FLT is also used by Federal Reserve staff to analyze merger and acquisition applications submitted to the Board by financial institutions.

1. Information concerning individuals that is being collected and/or maintained.

Some of the information collected in FLT can directly identify a person. The majority of the data fields do not contain personally identifiable information; however, they can be combined to create personally identifiable information. Certain data elements, as indicated below, are required for analysis, while others are optional. The optional data fields are those that the institutions opt to provide to the examiner. The following data fields represent the potentially personally identifiable information stored in FLT.

- a. Borrower name (optional);
- b. Borrower identification number (optional);
- c. Home address (optional);
- d. Borrower gender (required);
- e. Borrower ethnicity (required);
- f. Borrower race (required);
- g. Loan identification/application number (required);
- h. Application date (required); and

- i. Geographic identifiers such as city, state, county, Metropolitan Statistical Area/Metropolitan Division, tract code, latitude, and longitude (required).

Additionally, Federal Reserve staff may also import custom loan data into FLT, usually in the form of extended HMDA or CRA data provided by banks, although it can potentially include other loan data such as auto loans or the location of payday loan locations. This data, when combined with other data fields, may also constitute personally identifiable information, such as:

- j. Annual Percentage Rate of a given loan;
- k. Borrower FICO scores; and
- l. Loan origination fees.

2. Source(s) of each category of information listed in item 1.

The personally identifiable information maintained in FLT is primarily collected by Federal Reserve staff either in electronic form directly from financial institutions or manually from their loan files during the course of a Federal Reserve consumer compliance examination of that institution. However, some of the information is also collected from data submitted to the Board by lending institutions, which are required under the Board's HMDA Regulation to submit their HMDA lending data to the Board on an annual basis.

3. Purposes for which the information is being collected

Federal Reserve CCS staff use FLT on all consumer compliance examinations of financial institutions for the purpose of CRA and fair lending data analysis and compliance with applicable laws and regulations. Analysis of applicable data during the course of a consumer compliance examination allows the Federal Reserve to determine if an institution is meeting the credit and lending needs of its defined market. If an institution's performance is below satisfactory or in non-compliance, in-depth record-by-record data analysis can provide insight to the problem areas. Federal Reserve staff also use FLT to analyze data submitted to the FFIEC by financial institutions to assess financial institutions' compliance with the Board's HMDA and CRA regulations and the Board's overall HMDA data analysis. Finally, FLT is also used by Federal Reserve staff to analyze merger and acquisition applications submitted to the Board by financial institutions.

4. Who will have access to the information.

Access to data by a user within the Federal Reserve is limited to authorized employees within the Federal Reserve who have a need for the information for official business purposes. However, the information maintained in FLT may be subject to disclosure under the Freedom of Information Act or in connection with fair lending cases that may be referred to the U.S. Department of Justice. In addition, the information in FLT may be disclosed for enforcement, statutory and regulatory purposes; to another agency or a Federal Reserve Bank; to a member of Congress; to the Department of Justice, a court, an adjudicative body or administrative tribunal, or a party in litigation; to contractors, agents, and others; and where security or confidentiality has been compromised to prevent, minimize, or remedy such harm that may occur.

5. Whether the individuals to whom the information pertains will have an opportunity to decline to provide the information or consent to particular uses of the information (other than required or authorized uses).

Individuals do not have an opportunity to decline to provide the information or consent to particular uses of the information.

6. Procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date.

As previously discussed, the personally identifiable information maintained in FLT is collected directly from the lending records of financial institutions. FLT is designed to use the most current and complete CRA and HMDA data available. CRA data is collected from a financial institution at the start of an examination. The HMDA data are updated on a weekly basis with the most current data submissions from financial institutions.

The FLT data import process incorporates FFIEC data verification edits that check for quality and validity errors. Quality edits check for missing income, revenue and loan amount information. Validity edits check for missing or invalid geographic identification information. Records that fail either or both edit checks can be manually corrected during the import process or written to an error file for correction. FLT also includes sampling functionality that creates a random sample of loan records based on CRA and HMDA loan sampling requirements. Randomly selected loan records are used to verify content of loan records in accordance with established data verification procedures. Corrections to incomplete or inaccurate

records are either made by the institution or by the examiners on-site at the institution.

7. The length of time the identifiable information will be retained and how it will be purged.

Storage, retention and/or disposal of these files are compliant with the Board's applicable records retention authority (N1-82-00-02, Exam and Inspection Workpapers) and Federal Reserve System policies governing the use of electronic examination data. Lending data in FLT that contains identifiable information is retained for the duration of an examination. Once the examination is concluded, the lending data is retained for a minimum of six years or in accordance with examination frequency and trend analysis requirements, whichever is longer. Any paper documents are destroyed by shredding and electronic documents are purged from the appropriate databases after the retention period expires.

8. The administrative and technological procedures used to secure the information against unauthorized access.

FLT access is only granted to authorized Federal Reserve staff with a legitimate business need to use the tool. Federal Reserve staff must receive authorization from their Division Officer to gain access to FLT. Once the user has been approved, the system administrator is responsible for implementing the user's FLT access. FLT installations conform to Federal Information Security Management Act and Board authentication requirements applicable to mobile applications and data. This technology ensures that only the authorized user or system administrator has access to the FLT software product and associated lending data. The application is protected from installation and use by two layer authentication. All data transmitted between the servers and the client computers is either done over the Board trusted network or the secure encrypted VPN. All personally identifiable information loaded into the Fair Lending Tool system is stored on Board secure servers. The Fair Lending Tool desktop application can only be accessed on Board authorized, password protected laptop computers with fully encrypted hard disk drives.

9. Whether a new system of records under the Privacy Act be created. (If the data is retrieved by name, unique number, or other identifier assigned to an individual, then a Privacy Act system of records may be created).

FLT does not require publication of a system of records under the Privacy Act

since personally identifiable information is not retrieved by reference to an individual's name or other personal identifier.

Reviewed:

Charles S. Struckmeyer */signed/*

09/16/2010

Chief Privacy Officer

Date

Maureen Hannan */signed/*

09/16/2010

Chief Information Officer

Date