

USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: USDA Rural Development

System Name: Consumer

System Type: **Major Application**
 General Support System
 Non-major Application

System Categorization (per FIPS 199): **High**
 Moderate
 Low

Description of the System:

The three main components of Consumer are –UniFi Loan Origination System, – Fiserv - Loan Servicing Platform (formerly the MortgageServ Loans Servicing application), and National Office Reserve Funds (NORF) Web Application. The Consumer systems process borrower loan origination and loan servicing data. The Consumer loan origination system supports loan prequalification, loan application tracking, processing, and closing activities. The field office staff primarily handles these activities. The loan servicing system provides standard mortgage servicing processes, such as escrow accounts for taxes and insurance, forced-placed insurance, pre-determined amortization schedules, and default management.

Rural Development purchased UniFi and FiServ - Loan Servicing Platform to originate and service direct Consumer loans and grants for the newly established Centralized Servicing Center (CSC) in St. Louis, Missouri. This system was significantly enhanced to accommodate the unique requirements of the Consumer loan programs. Implementation of FiServ – Loan Servicing Platform brought new servicing capabilities to the Agency such as escrowing, forced-placed insurance, and pre-determined amortization schedules. The FiServ – Loan Servicing Platform component also provides the interface to the U.S. Department of Treasury for the Treasury Offset Program and Cross Servicing for Guaranteed Loss Claims and provides the capability for lender monitoring.

Interfaces to Xerox and Pitney-Bowes automated mail processing applications and equipment which comprise the Automated Mail Processing (AMP) have also been developed which are used for direct mailings to borrowers for such items as monthly billing statements and delinquency notices.

The Consumer System also includes the NORF Web Application, providing web pages for the State Offices to input requests for funds reserves from the National Office. The application includes web pages for the State Offices to view the status of requests for funding and pages for the National Office staff to view or process these requests.

Internal users of the Consumer Systems are the CSC, the Office of the Deputy Chief Financial Officer (DCFO) located in St. Louis, Missouri, and National Office, and State and local servicing

USDA PRIVACY IMPACT ASSESSMENT FORM

offices across the nation. External users include the U.S. Department of Treasury, Internal Revenue Service, tax services, insurance companies, credit bureaus, and commercial banks providing lockbox services.

Who owns this system?

Janet Havelka
USDA Rural Development
4300 Goodfellow Blvd.
St. Louis, MO 63120
Janet.havelka@stl.usda.gov
(314) 457-4980

Who is the security contact for this system?

Eugene Texter
USDA Rural Development
Building 105, FC-44
4300 Goodfellow Boulevard
St. Louis, MO 63120
eugene.texter@stl.usda.gov
314-457-4778

Brenda Dinges
USDA Rural Development
Building 105, FC-44
4300 Goodfellow Boulevard
St. Louis, MO 63120
brenda.dinges@stl.usda.gov
314-457-4772

Who completed this document?

Susan Self
USDA Rural Development
4300 Goodfellow Blvd.
St. Louis, MO 63120
Susan.self@stl.usda.gov
(314) 457-4988

USDA PRIVACY IMPACT ASSESSMENT FORM

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

QUESTION 1	Citizens	Employees
Does the system contain any of the following type of data as it relates to individual:		
Name	Yes	Yes
Social Security Number	Yes	No
Telephone Number	Yes	Yes
Email address	Yes	Yes
Street address	Yes	No
Financial data (i.e. account numbers, tax ids, etc)	Yes	No
Health data	No	No
Biometric data	No	No
QUESTION 2		
Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.?	Yes	No
NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code ¹		
Are social security numbers embedded in any field?	Yes	No
Is any portion of a social security numbers used?	Yes	No
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	No	No



If all of the answers in Questions 1 and 2 are NO,
 You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:
No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

¹ Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

DATA COLLECTION

3. Generally describe the data to be used in the system.

Customer Information: Borrower and co-borrower names, social security numbers, addresses, financial data, debt payment information, and tax and hazard insurance information.

Employee Information: Employee name, work area and teller number.

Vendor Information: Vendor Identification Numbers, Vendor names, and addresses.

4. Is the collection of the data both relevant and necessary to the purpose for which the system is designed? In other words, the data is absolutely needed and has significant and bearing on the system's purpose.

- Yes
- No. If NO, go to question 5

4.1. Explain.

The data attributes is used to provide loan processing information.

5. Sources of the data in the system.

5.1. What data is being collected from citizens and/or employees?

Borrower and co-borrower names, social security numbers, addresses, financial data, debt payment information, and tax and hazard insurance information..

5.2. What USDA agencies are providing data for use in the system?

USDA Rural Development loan officers input loan origination and application data.
Centralized Servicing Center inputs vendor information and loan servicing information.

5.3. What government agencies (state, county, city, local, etc.) are providing data for use in the system?

The Federal Bankruptcy Courts provides files with debtor bankruptcy notices via the Defense Automated Addressing System Center (DAASC).

U.S. Department of Treasury provides files for delinquency management processes such as Treasury Offset Program and Cross Servicing.

No state or local agencies are providing data to the system.

5.4. From what other third party sources is data being collected?

Proctor Financial Insurance Company provides forced place insurance information. U.S. Bank provides borrower's loan payment information through lock box files. Transunion Credit Bureau provides credit reports and credit scores of potential and current borrowers. First American Real Estate Tax Service provides a file containing borrower real estate tax information as a service for some taxing authorities.

6. Will data be collected from sources outside your agency? For example, citizens and employees, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

- Yes – See # 5
 No. If NO, go to question 7

6.1. How will the data collected from citizens and employees be verified for accuracy, relevance, timeliness, and completeness?

Through daily system update and exception reports and daily audit reports.

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness? Same as 6.1 In addition, application software contains internal edits to ensure data integrity.

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness? Same as 6.1 In addition, application software contains internal edits to ensure data integrity.

DATA USE

7. Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?

The data is used to provide loan processing information.

8. Will the data be used for any other purpose?

- Yes
 No. If NO, go to question 9

8.1. What are the other purposes?

9. Is the use of the data both relevant and necessary to the purpose for which the system is being used? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose.

- Yes
 No. If NO, go to question 10

9.1. Explain.

The data is used to provide loan processing information.

10. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

- Yes
FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

No. If NO, go to question 11

11. Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?

The data is used to provide loan processing information.

12. Will the data be used for any other purpose (other than indicated in question 11)?

Yes
 No. If NO, go to question 13

12.1. What are the other purposes?

13. Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

Yes
 No. If NO, go to question 14

13.1. What controls are in place to protect the data and prevent unauthorized access?

1. The applications' capability to establish access control lists (ACL) or registers is based upon the basic security setup of the operating system.
2. Application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties via access given to user Ids limited to what is needed to perform their job.
3. The controls used to detect unauthorized transaction attempts are security logs/audit trails.
4. The National Information Technology Center (NITC) hosts the Fiserv – Loan Servicing Platform application on the mainframe. NITC forces an automatic lockout from the mainframe when the system detects a certain period of inactivity and users are forced to log on again.

All desktop PC's are pre-loaded by Information Technology Services (ITS) with a self locking security feature to prevent unauthorized access to systems. The feature automatically locks the PC after a period of inactivity.

In addition, all employees have been trained and instructed to manually lock their PC's when leaving their workstations.

Warning banners are used to warn and inform users who sign on to the system that this is a secure and private network. Warning banners are in compliance with USDA guidelines.

FOR OFFICIAL USE ONLY

14. Are processes being consolidated?

- Yes
 No. If NO, go to question 15

14.1. What controls are in place to protect the data and prevent unauthorized access?

The controls in question 13.1 still apply.

DATA RETENTION

15. Is the data periodically purged from the system?

- Yes
 No

15.1. How long is the data retained whether it is on paper, electronically, in the system or in a backup?

Loan history is retained on-line for 48 months. Tape backups of all data are stored for 15 years. Loan origination information is kept on the system for the life of the loan.

15.2. What are the procedures for purging the data at the end of the retention period?

Once data is no longer needed, it is properly destroyed. Methods such as overwriting the entire media, degausses, and disk formatting are used, but strict attention is paid to whatever process is selected to ensure that all unneeded data is completely destroyed. Papers and other soft materials, such as microfiche and floppy disks, are shredded.

15.3. Where are these procedures documented?

Procedures for purging loan history are documented in Latitude, the Fiserv – Loan Servicing Platform on-line documentation.

16. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

Through daily system update and exception reports and daily audit reports.

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

- Yes – See # 15
 No

DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

- Yes
- No

18.1. How will the data be used by the other agency?

General Accounting Office (GAO) and Office of Inspector General (OIG) may be given limited access the data for oversight and auditing purposes. Data files are exchanged with the National Finance Center (NFC) for certain disbursements associated with a loan. A file is sent to the NFC to disburse the funds, then NFC returns a file with disbursement details to update the loans.

18.2. Who is responsible for assuring the other agency properly uses of the data?

The System Owner

19. Is the data transmitted to another agency or an independent site?

- Yes
- No. If NO, go to question 20

19.1. Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

Yes. Interconnection Service agreements and Memorandum of understanding are in place for data transmissions

19.2. Where are those documents located?

ISA and MOUs are maintained by the ISSS team and available upon request.

20. Is the system operated in more than one site?

The FiServ – Loan Servicing Platform application is hosted on a mainframe computer. The UniFi and NORF applications are hosted on web farm servers located in Kansas City. Access is through user terminals, which are on the USDA network.

20.1. How will consistent use of the system and data be maintained in all sites?

USDA policies and procedures, as well as federal regulations, ensure that the data is used in a consistent manner across the agency. User training manuals, handbooks, policy letters, etc., are posted on a central web site for access by all users. Discretionary access controls based on need to know are also employed to help maintain consistency across the agency.

DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

USDA Rural Development system users and managers, Rural Development Systems Administrators, developers, and analysts and contractors.

22. How will user access to the data be determined?

Access is given on a 'need-to-know' basis.

22.1. Are criteria, procedures, controls, and responsibilities regarding user access documented?

- Yes
- No. If NO, go to question 23

22.2. Where are criteria, procedures, controls, and responsibilities regarding user access documented?

Criteria, procedures, controls, and responsibilities are documented in the system SSP, the Trusted Facilities Manual, and the Secure Facility User's Guide.

23. How will user access to the data be restricted?

Privileges granted are based on job functions and area of authority (e.g., State office user with authority for their state only).

23.1. Are procedures in place to detect or deter browsing?

- Yes – See description below
- No

23.2. Are procedures in place to detect or deter unauthorized user access?

- Yes – See description below
- No

1. Application users are restricted from accessing the operating system, other applications, or other system resources based on the access roles that were assigned to them when issued their user id
2. The controls used to detect unauthorized transaction attempts are security logs/audit trails. Audit mechanisms exist at both the OS and application level for FiServ – Loan Servicing Platform. Any UniFi events may be captured by Microsoft Windows 2003 and NORF events may be captured by Microsoft Windows 2000. FiServ – Loan Servicing Platform provides numerous daily auditing reports for managers to monitor user activity within the application.
3. For FiServ – Loan Servicing Platform, NITC forces an automatic lockout from the mainframe when the system detects a certain period of inactivity and users are forced to

USDA PRIVACY IMPACT ASSESSMENT FORM

log on again. UniFi also forces an automatic lockout from the production servers after a certain period of inactivity and users are forced to log on again.

4. All desktop PC's are pre-loaded by ITS with a self locking security feature to prevent unauthorized access to systems. The feature automatically locks the PC after a period of inactivity. In addition, all employees have been trained and instructed to manually lock their PCS's when leaving their workstations.

Warning banners are used to warn and inform users who sign on to the system that this is a secure and private network. Warning banners are in compliance with USDA guidelines.

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

- Yes – See above
 No

CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the citizens and employees affected by the interface (i.e. office, person, departmental position, etc.)?

Janet Havelka
Chief, Mortgage Loan Technologies Branch
Building 104, FC-425
4300 Goodfellow Boulevard St. Louis, MO
Office: 314-457-5012
Janet.Havelka@stl.usda.gov

26. How can citizens and employees contact the office or person responsible for protecting their privacy rights?

Citizens and employees may contact the Freedom of Information Officer:

Dorothy Hinden
Freedom of Information Officer
Rural Development, USDA
7th Floor, Reporter's Bldg.
Washington, DC 20250
Dorothy.Hinden@wdc.usda.gov
(202)692-0031

27. A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

- Yes - If YES, where is the breach notification policy located?

- U.S. Department of Agriculture Incident Notification Plan September 2007

- DM3505-001 USDA Computer Incident Response Procedures Manual.

- Computer Incident Response Standard Operating Procedures (CIRT)

FOR OFFICIAL USE ONLY

USDA PRIVACY IMPACT ASSESSMENT FORM

28. Consider the following:

- Consolidation and linkage of files and systems
- Derivation of data
- Accelerated information processing and decision making
- Use of new technologies

Is there a potential to deprive citizens and employees of fundamental rules of fairness (those protections found in the Bill of Rights)?

- Yes
 No. If NO, go to question 29

28.1. Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of citizens and employees?

DM 3515-002, section e states:

To fulfill the commitment of the USDA to protect customer and employee data, several issues must be addressed with respect to privacy:

- 1 The use of information must be controlled; and
- 2 Information may be used only for a necessary and lawful purpose.

Where Public Affairs systems of records are involved:

- 1 Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them;
- 2 Information collected for a particular purpose should not be used for another purpose without the subject's consent unless such other uses are specifically authorized or mandated by law; and
- 3 Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

Also, P.L. 95-454, the Civil Service Reform Act of 1978 which is enforced by The U.S. Equal Employment Opportunity Commission (EEOC) ensures the equitable treatment of the employees.

30. Is there any possibility of treating citizens and employees differently and unfairly based upon their individual or group characteristics?

- Yes
 No. If NO, go to question 31

30.1. Explain
Non Applicable

FOR OFFICIAL USE ONLY

SYSTEM OF RECORD

31. Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

- Yes
 No

31.1. How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

FiServ – Loan Servicing Platform -

Stores borrower name, address, social security number, loan number, and telephone number. The cross reference feature in FiServ – Loan Servicing Platform allows users to search on any of the listed criteria for the particular borrower record, as well as Flood Tracking Number where applicable.

UniFi -

Stores much the same information as FiServ – Loan Servicing Platform. Application information can be retrieved by application #, name, or social security.

NORF -

Stores the date of the requested funds, the borrower name, account number, amount requested, and loan program type. Data cannot be retrieved by personal identifier. All reports are based on the date the request for funds was entered. Criteria can be a single date or a date range.

31.2. Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov).

USDA/RURAL DEVELOPMENT-1

31.3. If the system is being modified, will the SOR require amendment or revision?

Modifications to the system will be recorded as part of the Configuration Management process and major revisions will be reflected in updates of the Certification and Accreditation documentation and, if deemed necessary, will trigger re-accreditation of the system.

Rural Development’s SDLC and CM process requires the ISSS to review system changes for security documentation updates and re-accreditation decisions impact to ensure that the system SORN is revised as needed.

TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

- Yes
 No. If NO, the questionnaire is complete.

32.1. How does the use of this technology affect citizens and employees privacy?
N/A

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO
THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE/CYBER SECURITY

USDA PRIVACY IMPACT ASSESSMENT FORM

Privacy Impact Assessment Authorization
Memorandum

I have carefully assessed the Privacy Impact Assessment for the Consumer System

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.



System Manager/Owner



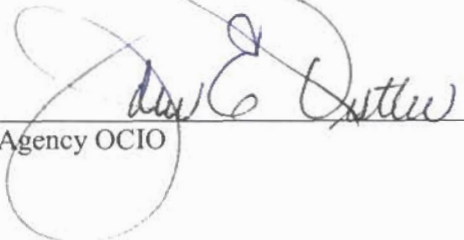
Date



Brenda Dinges - Agency's Chief FOIA Officer



Date



Agency OCIO



Date

FOR OFFICIAL USE ONLY