

## USDA PRIVACY IMPACT ASSESSMENT FORM

**Agency:** Food and Nutrition Service

**System Name:** Anti-Fraud Locator using EBT Retailer Transactions (ALERT)

**System Type:** Non-major Application

**System Categorization (per FIPS 199):**

{(Confidentiality, HIGH), (Integrity, MODERATE),  
(Availability, MODERATE)}

### Description of the System:

FNS has the primary responsibility for monitoring any fraudulent activity by retailers and the individual States for recipients. While traditional methods of fraud, identified under the coupon distribution/redemption system, are reduced through the use of EBT, the nature of electronic transactions also introduces previously unknown approaches to committing fraud. Methods of detecting (and ultimately preventing) food stamp fraud by EBT enabled retailers are essential to the successful management of the benefit redemption process.

The ALERT system receives daily transaction records from EBT processors and conducts analysis of patterns in the data, which indicate potential fraudulent activity by stores. FNS investigators and compliance offices use these reports to support case management. Other users include USDA Office of the Inspector General (OIG) investigators and the staff members of Regional and Field offices.

ALERT system managers and developers constantly review program experience with trafficking issues and develop new detection patterns for the scanning software suite.

**Who owns this system?** (Name, agency, contact information)

**Andrea Gold**  
**Food and Nutrition Service**  
**Benefit Redemption Division (BRD)**  
**(703) 305-2456**

**Who is the security contact for this system?** (Name, agency, contact information)

**Gene Beasley**

USDA PRIVACY IMPACT ASSESSMENT FORM

**USDA/FNS/BRSB**  
**45 S. 7<sup>th</sup> Street, Suite 1810**  
**Minneapolis, MN 55402**  
**(612) 370-3350**

**Who completed this document? (Name, agency, contact information)**

**John Coulter**  
**USDA/FNS/BRSB**  
**45 S. 7<sup>th</sup> Street, Suite 1810**  
**Minneapolis, MN 55402**  
**(612) 370-3354**

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

Indicate whether the following types of personal data are present in the system

<b>QUESTION 1</b>	Citizens	Employees
Does the system contain any of the following type of data as it relates to individual:		
Name	N	N
Social Security Number	N	N
Telephone Number	N	N
Email address	N	N
Street address	Y	Y
Financial data	Y	Y
Health data	N	N
Biometric data	N	N
<b>QUESTION 2</b>	N	N
Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.?		
NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code <sup>1</sup>		
Are social security numbers embedded in any field?	N	N
Is any portion of a social security numbers used?	N	N
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	N	N



**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:

**3. 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.

<sup>1</sup> 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.

ALERT collects store address information and financial transaction information of stores. ALERT also collects Household ID and Electronic Benefit Transfer (EBT) Card Numbers but these are created by State agencies and there is no automated way for ALERT to know the identity of the EBT card holder.

4. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

Yes

5. Sources of the data in the system.

5.1. What data is being collected from the customer?

Financial store transactions.

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

FNS only

5.3. What state and local agencies are providing data for use in the system?

None.

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

Electronic Benefit Transfer (EBT) processors provide daily redemption information for each store in the program that has redemptions. Store information including store address is taken from the STARS system. Mapping data is purchased and Bureau of Census demographic data is purchased. On an ad hoc basis, FNS has obtained additional recipient data from State Agencies for research and special emergency evaluation circumstances.

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

Yes

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

N/A No data is received from customers.

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

Store transaction data is collected daily from EBT processors. Monthly summary data is also provided and used to verify the daily transaction data. Store address is verified by the STARS system.

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?

Information from the STARS system is verified by STARS.

## 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?

There is no customer information in ALERT. Financial transaction data is used to determine signs of fraud or abuse of the Food Stamp Program.

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

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 designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President

Yes

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.)?

USDA PRIVACY IMPACT ASSESSMENT FORM

No – stores only

10.1. Will the new data be placed in the individual's record (customer or employee)?

10.2. Can the system make determinations about customers or employees that would not be possible without the new data?

10.3. How will the new data be verified for relevance and accuracy?

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?

Financial transaction data is used to determine signs of fraud or abuse of the Food Stamp Program.

12. Will the data be used for any other uses (routine or otherwise)?

No. If NO, go to question 13

12.1. What are the other uses?

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, data is being consolidated from the STARS and EBT processors. These systems provide financial analysis of transactions in order to detect cases of fraud and abuse of the FSP.

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

Access to privacy information is strictly controlled by role based log-in information. In addition data is encrypted in transit.

14. Are processes being consolidated?

No. If NO, go to question 15

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

## DATA RETENTION

15. Is the data periodically purged from the system?

No. If NO, go to question 16

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

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

15.3. Where are these procedures documented?

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?

Financial daily transactions are compared with monthly summary data to ensure the data is accurate.

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

Yes

## 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, state agencies.

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

States also use this data to detect fraud and abuse of the Food Stamp Program.

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

The shared data does not contain privacy information on customers. Access to the system is controlled by FNS through the authorization process.

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

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?

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

Yes

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

The system is designed to be used across all sites with the same role-based access controls and safeguards at all sites.

## DATA ACCESS

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

Access is limited to FNS staff and managers responsible for store authorization, store monitoring and FNS compliance investigators.

In addition, USDA/OIG investigators and managers have access. Access beyond those is very limited and includes contracted developers and testers.

USDA and FNS employees in general do not have access. ALERT is an investigative system and access is strictly



limited to those who have an approved need to know.

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

Need to know. Access and access controls are documented.

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

Yes.

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

Users are restricted to their areas of assigned responsibilities.

**23.1. Are procedures in place to detect or deter browsing or unauthorized user access?**

Yes.

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

Yes – HTTPS is used for encryption in transmission. eAuthentication will be used for authentication of users.

## **CUSTOMER PROTECTION**

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

**Andrea Gold  
Food and Nutrition Service  
Benefit Redemption Division (BRD)  
(703) 305-2456**

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

They can contact their local field or regional office.

**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

27.1. If NO, please enter the POAM number with the estimated completion date:

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 a customer of due process rights (fundamental rules of fairness)?

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 customers?

By analyzing EBT data and going by the numbers only, ALERT does not discriminate.

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

No. If NO, go to question 31

30.1. Explain

## **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?

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.)?

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](http://www.access.GPO.gov))

USDA/FNS-9, Food Stamp Program Retailer Information,  
Federal register vol. 64, No 64, Monday, April 12, 1999

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

NO

## TECHNOLOGY

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

No. If NO, the questionnaire is complete.

32.1. How does the use of this technology affect customer privacy?

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

## Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

ALERT  
\_\_\_\_\_  
(System Name)

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  
OR Project Representative  
OR Program/Office Head. \_\_\_\_\_  
Date

\_\_\_\_\_  
Agency's Chief FOIA officer  
OR Senior Official for Privacy  
OR Designated privacy person \_\_\_\_\_  
Date

\_\_\_\_\_  
Agency OCIO \_\_\_\_\_  
Date


## Privacy Impact Assessment Authorization Memorandum

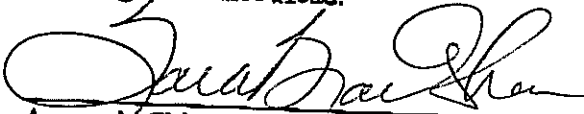
I have carefully assessed the Privacy Impact Assessment for the

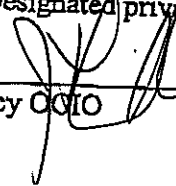
ALERT  
(System Name)

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  
OR Project Representative  
OR Program/Office Head. 6/29/07  
Date

  
\_\_\_\_\_  
Agency's Chief FOIA officer  
OR Senior Official for Privacy  
OR Designated privacy person 7/2/07  
Date

  
\_\_\_\_\_  
Agency OCIO FDR 7/2/07  
Date