Privacy Impact Assessment

Anti-Fraud Locator using EBT Retailer Transaction (ALERT)

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: April 14, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

Anti-Fraud Locator using EBT Retailer Transaction

(ALERT)

Contact Point

Ambur Daley
OIT/PMD/PMB
United States Department of Agriculture
(703) 305-2125

Reviewing Official

Miguel Marling
Privacy Officer
United States Department of Agriculture
Miguel.Marling@usda.gov

Bianca O'Hare
ISO/ISSM
United States Department of Agriculture
(703) 605-1534

Document Review

Name	Title	Date	Comments
Miguel Marling	FNS Privacy Officer	4/28/2020	

SUMMARY INFORMATION	
Date	April 14, 2020
Name of Project	Anti-Fraud Locator using EBT Retailer Transaction (ALERT)
Name of Component:	FNS/OIT/PMB
Name of Information Owner/Steward:	Andrea Gold / Linda Sung-Lee
Phone of Information Owner/Steward:	703-305-2434 / 949-232-1177
Email of Information Owner/Steward:	andrea.gold@usda.gov / linda.sung-lee@usda.gov
Name of Project Manager:	Ambur Daley
Phone for Project Manager:	703-305-2125
Email for Project Manager:	ambur.daley@usda.gov
Name of System Owner:	Vance Parker
Phone for System Owner:	703-305-2777
Email for System Owner:	vance.parker@usda.gov

Abstract

Anti-Fraud Locator Using Electronic Benefits Transfer (EBT) Retailer Transactions (ALERT). ALERT has the primary responsibility for monitoring any fraudulent activity by retailers and the individual States for recipients. Due to findings in the Privacy Threshold Analysis for ALERT, a Privacy Impact Assessment is warranted.

Overview

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 may indicate potential fraudulent activity by stores. FNS investigators and compliance offices use these reports to distinguish between Stores whose ALERT data is strongly suggestive of violations and Stores whose ALERT data may be explained through legitimate business practices. If determination is made for EBT case processing, an EBT case is initiated and evidence is collected in the Case Analysis Document to support case management. Other users include the USDA Office of the Inspector General (OIG) investigators.

ALERT system managers and developers constantly review program experience with trafficking issues and develop new detection patterns for the scanning software suite. ALERT shares information on retailers with the Store Tracking and Redemption System (STARS). ALERT is owned by the SNAP Retailer Policy and Management Division (RPMD), Retailer Administration Branch (RAB). The business point of contact is Linda Sung-Lee, Acting Chief, RAB.

In 2013, the ALERT Data Mining environment was added to the system boundaries of the ALERT system. The ALERT Data Mining integrates EBT transaction data from ALERT and Retailer data from STARS. The data is refreshed on an as-needed basis through data extracts received from backups. The data from these sources is stored on an isolated server and available only to approved Data Miners and not accessible by ALERT users.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

ALERT collects EBT transaction data for Retailers in the SNAP program received from the EBT processors. The EBT transactions include the *household_account_number* and Electronic Benefits Transfer (EBT) Card Number. The *household_account_number* is assigned by the States, and some States use the SSN as the *household_account_number*. There is no automated way for ALERT to know the identity of the EBT card holder. ALERT also collects Store data from the STARS system.

ALERT scans the EBT transaction data combined with the Store data to detect patterns of behavior that might indicate fraud. The suspicious EBT transactions are flagged for review. FNS investigators and compliance offices use various ALERT reports to distinguish between Stores whose ALERT data is strongly suggestive of violations and Stores whose ALERT data may be explained through legitimate business practices. If determination is made for EBT case processing, an EBT case is initiated and evidence is collected in the Case Analysis Document to support case management. The Case Analysis Document is used to capture evidence against the Store and maintained in the centralized Alfresco Library for FNS. ALERT creates charge letters against the Store that include attachments of transactions to be used as evidence in a case against the Store. The Charge Letter is transferred to the STARS system.

The ALERT Data Mining integrates EBT transaction data from ALERT and Retailer data from STARS.

Financial Data - Store financial transactions are received from the Electronic Benefits Transfer processors from each State. This contains EBT Card Numbers and Household Account Numbers, which for some states, may contain the SSN of the card holder. Electronic

Benefits Transfer (EBT) processors provide daily redemption information for each store in the program that has redemptions.

Miscellaneous Identification Number - The data received from the EBT processors contains a state agency assigned number and/or case number.

1.2 What are the sources of the information in the system?

The data sources for the ALERT system are:

- EBT processors who send Retailer transaction data to ALERT: Store financial transactions are received from the Electronic Benefits Transfer processors from each State. This contains Household ID numbers which for some states may contain the SSN of the card holder. Electronic Benefits Transfer (EBT) processors provide daily redemption information for each store in the program that has redemptions.
- STARS system that provides Store and case related data: Store address and Case data is replicated from the STARS system.
- ESRI: ALERT interfaces with ESRI for geospatial maps, locator and routing services through an online subscription.
- ZIP Code data from Zip-Codes.com: The zip code data is obtained from the Zip-Code.com subscription at the beginning of each month. This data is used to determine the time zone and daylight savings status for retailers based on their zip code.

The data sources for the ALERT Data Mining are ALERT and STARS.

1.3 Why is the information being collected, used, disseminated, or maintained?

The principal purpose of the information collected by the ALERT system is to enable the Retailer Policy and Management Division (RPMD) and the Retailer Administration Branch (RAB) staff to detect fraud or abuse of the SNAP program. The only PII data included in the EBT transaction is the *household_account_number* which for some States may contain SSN. This is used only for reference to State agency data that uniquely identifies the SNAP recipient household.

This data is not collected directly by ALERT. It is collected by Stores through transactions made by the individual at the Store using the EBT Card. The Store redemption transactions are forwarded to ALERT by the EBT processors.

The data collected for the ALERT Data Mining is for the purpose of detecting new patterns of behavior that may be indicative of fraud. The new patterns may then be implemented in the ALERT system to scan the EBT transaction data.

1.4 How is the information collected?

Information is collected from store financial transactions - this is received from the Electronic Benefits Transfer (EBT) processors from each state. EBT processors provide daily redemption information for each store in the program that has redemptions. EBT processors are responsible for delivering a daily submission properly formatted for each of the states that they service. These files are contained within a compressed file (zip file) that is used to transfer the data via network. The compressed file includes the submission files. Each EBT submission file contains a single header record followed by one or more EBT transaction records, followed by a single trailer record. A submission file contains all of the transactions conducted by recipients of the serviced State regardless of what State the retailer resides in. ALERT uses an Extract, Transform and Load (ETL) process to validate and load the data. Business intelligence is then applied to this data for fraud detection purposes.

Store information, including store address is replicated from the STARS system. The replication of the Store, Watch List, and Case data from the STARS Database to the STARS Replication Database is performed via a subscription process whereby the STARS Replication Database continuously pulls data from an intermediate distribution database where selected STARS data has been published. The replicated data is then transformed and loaded into the ALERT Data Repository. Data stored in the ALERT Data Repository is subsequently used to feed the ALERT Data Mart.

The Mapping, locator, and routing data services are purchased from ESRI. Mapping provides base maps on which the ALERT data is overlaid. The locator service can be used to geocode single addresses, reverse geocode, or batch geocode addresses. The Routing service enables the generation of routes and driving directions form two or more points in the United States and Canada.

The zip code data is obtained from the Zip-Code.com subscription at the beginning of each month. The zip code data is downloaded, prepared, and uploaded into the ALERT databases in all ALERT environments (Production, UAT, Integration, etc.). This data is used to determine the time zone and daylight savings status for retailers based on their zip code.

The ALERT Data Mining integrates EBT transaction data from ALERT and Retailer data from STARS. The data is refreshed on an as-needed basis through data extracts received from backups. The data from these sources is stored on an isolated server and available only to approved Data Miners.

1.5 How will the information be checked for accuracy?

The EBT transaction submission files received from the EBT processors are checked, validated, and loaded into the ALERT database based on defined validation rules. The validation process checks for valid filename, file layout, header/trailer records, record lengths, record count etc. Financial daily transactions are compared with monthly summary data to ensure the data is accurate.

Store data is verified by the STARS system and replicated into the ALERT system through an ETL process.

The source systems (ALERT and STARS) are responsible for the accuracy of the data used for ALERT Data Mining.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Food and Nutrition Act of 2008. Information is required by Public Law 110-246, The Food, Conservation and Energy Act of 2008 (FECA).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Access to ALERT functionality is granted based on user role. Users are restricted to their areas of assigned responsibilities. Access is limited to FNS field staff/managers involved in case screening and case analysis, FNS compliance investigators, USDA OIG investigators and managers, as well as operations support personnel. Other USDA and FNS employees do not have access.

PII data is encrypted at rest and in transit. The *household_account_number* is stored in the ALERT database as an encrypted field. This data is masked when included in the Final Charge Letter.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

ALERT combines data from various sources to look for patterns of fraud and abuse. ALERT passes "Watch List" data to the STARS system. Users of the ALERT system can review transactions to determine if there is a reasonable explanation for the suspicious activity or if the transactions are signs of fraud.

In 2013, the ALERT Data Mining environment was added to the system boundaries of the ALERT system. This effort includes data from ALERT and STARS. This data is only available to approved data miners and not to general ALERT users.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Microsoft SQL Server is used to analyze data and detect new fraudulent data patterns.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

ALERT uses commercially available geospatial data from ESRI. The ESRI base map is used to plot Stores on a map and generate optimum route between selected points on the map.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

eAuthentication (Level 2) is used by authorized users to access the system. Users are assigned roles and constraints within the system that limit their access to data. The PII data is encrypted at rest and in transit.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

ALERT will have at least five years of data in the data mart (this is what is accessed by and available to the ALERT system itself) and at least seven years of data in the data repository, and the data files themselves are kept indefinitely.

For the ALERT Data Mining project, the data collected will be held until no longer needed.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. N1-462-09-12

For the data mining project, data is only held temporarily.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

There are no risks associated with the length of time data is retained.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Primary users are FNS staff and managers responsible for store authorization, store monitoring, as well as FNS and USDA/OIG compliance investigators. The information is used to detect patterns of behavior that might indicate fraud or abuse of the SNAP program.

4.2 How is the information transmitted or disclosed?

Information is retrieved through ALERT web pages using HTTPS.

For the Data Mining Project, only data miners have access to the data. They produce reports of possible ways of detecting fraud and abuse in the SNAP program. These reports do not contain any PII data but reveal how to detect fraud and abuse.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

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.

For the Data Mining Project, only approved data miners have access to the data.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

ALERT Data is only shared within the Department.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Privacy Act System of Records (SORN 9) – Food Stamp Program Retailer Information published December 27, 2010.

No PII information is shared outside the Department.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

No ALERT Data is shared outside the Department.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

No ALERT Data is shared outside the Department.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

http://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records

ALERT is FNS - 9 Privacy Act System of Records – Food Stamp Program Retailer Information published December 27, 2010.

6.2 Was notice provided to the individual prior to collection of information?

Not Applicable- The ALERT system, does not collect information directly from individuals but from financial institutions, therefore no notice is provided to individuals.

The only individual PII data is included in the EBT transaction data is the *household_account_number* which for some States may contain *SSN.* This is used only for reference to State agency data that uniquely identifies the SNAP recipient household. This data is not collected directly by ALERT. It is collected by Stores through transactions made by the individual at the Store using the EBT Card. The Store redemption transactions are forwarded to ALERT by the EBT processors.

For the ALERT Data Mining Project, all data comes from other FNS systems.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Not Applicable.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Not Applicable.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Not Applicable.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Not Applicable. This process is handled by the State Agency.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Not Applicable. This process is handled by the State Agency.

7.3 How are individuals notified of the procedures for correcting their information?

Not Applicable. This process is handled by the State Agency.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Not Applicable. This process is handled by the State Agency.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Not Applicable. This process is handled by the State Agency.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

See FNS Security Office for how users gain access to any FNS system. Each user must submit an FNS-674 form signed by their supervisor, the system owner, and FNS security officer before they are allowed access. Access is then granted through the ALERT system where appropriate roles and constraints are assigned.

For the ALERT Data Mining Project each data miner must submit an FNS-674 form signed by their supervisor, the system owner, and FNS security officer before they are allowed access.

8.2 Will Department contractors have access to the system?

Yes, for systems Operations and Maintenance purposes. The Data Mining Project team are all contractors.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Privacy training is a part of the annual security awareness training that all authorized users of USDA- FNS systems must complete before access to the system is granted.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. The ATO date is August 12, 2015

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Users of the system are audited at least annually. FNS-674 forms must be on file and their need to access the system is validated at least annually.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Because the only privacy item is the *household_account_numbe*r, which in some cases may contain social security numbers, and there are no other identifiable information, the risks are minimum. By controlling who has access and ensuring that they are given the least privileges needed to perform their job, FNS ensures that only valid users have access.

For the ALERT Data Mining only approved Data Miners have access to that data. FNS ensures that only valid Data Miners have access.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

The ALERT system is a web-based system. ALERT uses a three tier architecture. This includes a web server layer, an application server layer, and a database layer.

For the ALERT Data Mining project, there is only a database layer.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

Not Applicable.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

ALERT maintains a subscription with ESRI (ArcGIS Online) software API to provide geocoding services, routing (driving directions) services, and displaying locations on a map within ALERT.

ALERT leverages a service provided by US Census Bureau to look up Census Tract info for a given address.

ALERT uses a map layer provided by USDA ERS which displays an overview of food access indicators for low-income and other census tracts using different measures of supermarket accessibility.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

None.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not Applicable.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not Applicable.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not Applicable.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not Applicable.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not Applicable.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not Applicable.

10.10 Does the system use web measurement and customization technology?

No.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Not Applicable.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable.

Responsible Officials

AMBUR DALEY Digitally signed by AMBUR DALEY
Date: 2020.04.28 17:19:16 -04'00'

Ambur Daley
OIT/PMD/PMB
Food and Nutrition Service
United States Department of Agriculture

Date

JOSEPH BINNS Digitally signed by JOSEPH BINNS
Date: 2020.04.28 18:21:35 -04'00'

Joseph Binns
ISSPM/CISO
Food and Nutrition Service
United States Department of Agriculture

Date

Approval Signature

VANCE PARKER Digitally signed by VANCE PARKER
Date: 2020.05.01 19:03:29 -04'00'

Vance Parker
System Owner
Food and Nutrition Service
United States Department of Agriculture

Date